IFW

501.43790X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): D. NAKATSUKA

Serial No.: 10/828,287

Filed: April 21, 2004

Title: COMPUTER SYSTEM FOR ALLOCATING STORAGE AREA TO COMPUTER BASED ON SECURITY LEVEL

LETTER CLAIMING RIGHT OF PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

August 27, 2004

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on:

Japanese Patent Application No. 2004-052700
Filed: February 27, 2004

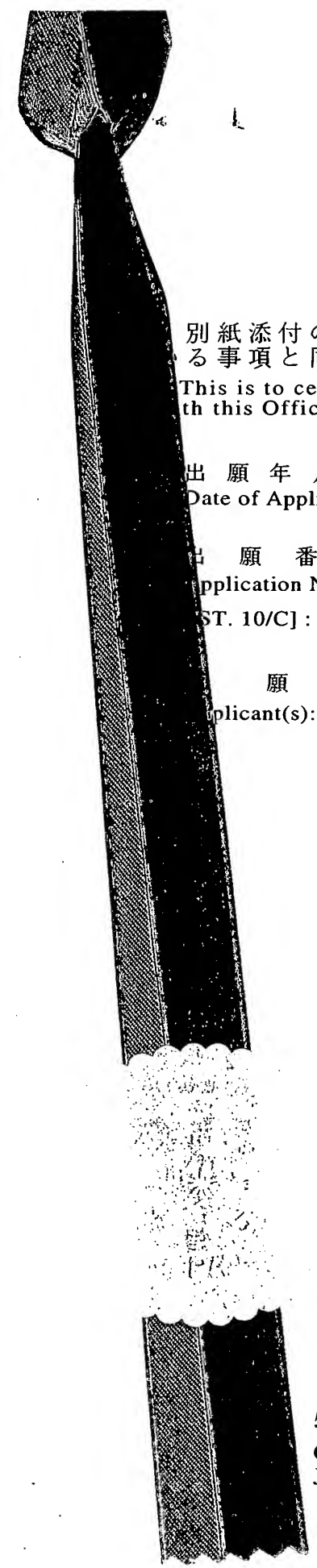
A certified copy of said Japanese Patent Application is attached.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Carl I. Brundidge
Registration No.: 29,621

CIB/rr
Attachment



CERTIFIED COPY OF
PRIORITY DOCUMENT

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月２７日

出願番号
Application Number: 特願２００４－０５２７００

[ST. 10/C]: [ＪＰ２００４－０５２７００]

願人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００４年　３月２４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０２４１８８

【書類名】　特許願
【整理番号】　K04000211A
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　中塚　大樹
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社　日立製作所
【代理人】
　【識別番号】　100075096
　【弁理士】
　【氏名又は名称】　作田　康夫
【選任した代理人】
　【識別番号】　100100310
　【弁理士】
　【氏名又は名称】　井上　学
【手数料の表示】
　【予納台帳番号】　013088
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
計算機と、
前記計算機とネットワークを介して接続される記憶装置システムと、
前記計算機及び前記記憶装置システムと接続される第二の計算機とを有し、
前記第二の計算機は、前記記憶装置システムに関する情報を有し、前記計算機の要求に基づいて、前記要求に合致する前記記憶装置システムを前記情報に基づいて選択し、前記選択された記憶装置システムに対して前記計算機が使用する記憶領域を前記計算機の要求に基づいて作成する指示を送信し、
前記記憶装置システムは、前記指示に従って前記計算機の要求を満たす記憶領域を作成し、作成終了を前記第二の計算機へ通知し、
前記第二の計算機は、前記通知の受領後、前記計算機へ前記記憶装置システムで作成された前記記憶領域に対する経路情報を通知することを特徴とする計算機システム。
【請求項２】
前記記憶装置システムに関する情報とは、前記記憶装置システムのセキュリティレベルに関する情報であり、
前記計算機の要求とは、高いセキュリティレベルが確保される記憶領域の作成の要求であることを特徴とする請求項１記載の計算機システム。
【請求項３】
前記セキュリティレベルに関する情報とは、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、
前記高いセキュリティレベルとは、前記装置がIPSec処理を行えるということであることを特徴とする請求項２記載の計算機システム。
【請求項４】
前記指示には、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える装置に前記記憶領域を対応付ける指示であり、
前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記装置に対応付け、
前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える前記装置に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項３記載の計算記システム。
【請求項５】
前記指示は、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える複数の装置に前記記憶領域を対応付ける指示であり、
前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記複数の装置に対応付け、
前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える前記複数の装置の個々に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項３記載の計算記システム。
【請求項６】
前記第二の計算機は更に、前記記憶装置システムが有する記憶領域を使用可能な前記ネットワークに接続された前記計算機の情報（以下「第二の情報」）を有し、
前記計算機は、前記第二の計算機に該計算機が使用できる記憶領域の情報の送付要求を発行し、
前記第二の計算機は、前記第二の情報に基づいて、前記計算機が使用できる前記記憶装置システムが有する前記記憶領域への経路情報を前記送付要求を発行した前記計算機に送信することを特徴とする請求項５記載の計算機システム。
【請求項７】
前記第二の計算機は、前記通知の受領後、前記計算機へ前記記憶装置システムで作成された前記記憶領域に対する経路情報を通知する際に、前記記憶領域の作成を要求した前記

計算機についての情報を前記第二の情報に登録することを特徴とする請求項６記載の計算機システム。

【請求項８】

前記記憶装置システムに関する情報とは、前記記憶装置システムのセキュリティレベルに関する情報であり、

前記計算機の要求とは記憶領域の作成の要求であり、

前記第二の計算機は、前記計算機が有するセキュリティレベルに応じて、前記記憶装置システムに前記記憶領域の作成を指示することを特徴とする請求項１記載の計算機システム。

【請求項９】

前記セキュリティレベルに関する情報とは、前記記憶装置システム又は前記計算機が前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記指示には、前記計算機が有するセキュリティレベルが前記IPSec処理を行える装置を有するレベルの場合に、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える装置に前記記憶領域を対応付ける指示であることを特徴とする請求項８記載の計算機システム。

【請求項１０】

前記記憶装置システムに関する情報とは、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記計算機の要求とは記憶領域の作成の要求であり、

前記第二の計算機は、前記記憶領域の作成の要求に基づいて、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える装置に対応付けて記憶領域を作成する指示を前記記憶装置システムに送信し、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記装置に対応付け、

前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える前記装置に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項１記載の計算記システム。

【請求項１１】

前記記憶装置システムに関する情報とは、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記計算機の要求とは、記憶領域の作成の要求であり、

前記第二の計算機は、前記記憶領域の作成の要求に基づいて、記憶領域を作成する指示を前記記憶装置システムに送信し、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える複数の前記装置に対応付け、

前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える複数の前記装置の各々に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項１記載の計算記システム。

【請求項１２】

前記記憶装置システムに関する情報とは、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報であり、

前記計算機の要求とは、記憶領域の作成の要求であり、

前記第二の計算機は、前記記憶領域の作成の要求に基づいて、記憶領域を作成する指示を前記記憶装置システムに送信し、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記装置及びIPSec処理を行えない前記装置とに対応付け、

前記第二の計算機は、前記計算機に、前記経路情報として、IPSec処理を行える前記装置に割り当てられた前記ネットワークにおけるアドレスの情報及びIPSec処理を行えない

前記装置に割り当てられた前記ネットワークにおけるアドレスの情報を通知することを特徴とする請求項１記載の計算記システム。

【請求項１３】

前記計算機は、前記第二の計算機から受信した前記複数のアドレスの情報から一つを選択して前記記憶装置システムが有する前記記憶領域へアクセスすることを特徴とする請求項１１及び１２に記載のうちいずれか一つの計算機システム。

【請求項１４】

前記計算機は、該計算機が行う処理が高いセキュリティレベルを必要とする場合には、前記複数のアドレス情報のうち、IPSec処理を行える前記装置に対応するアドレス情報を選択して前記記憶装置システムが有する前記記憶領域へアクセスすることを特徴とする請求項１３記載の計算機システム。

【請求項１５】

計算機及び記憶装置システムと接続される管理計算機であって、

制御部、メモリ及び前記計算機及び前記記憶装置システムと接続されるネットワークと接続されるインターフェースとを有し、

前記メモリは、ネットワークと接続される前記記憶装置システムが有する装置がIPSec処理を行えるかどうかを示す情報を有し、

前記計算機から前記記憶装置システムにおける記憶領域の作成が前記インターフェースを介して要求された際に、前記制御部は、前記要求に基づいて、IPSec処理を行える装置に対応付けるように前記記憶領域を作成する指示を前記記憶装置システムへ送信し、

前記記憶装置システムから完了通知を受領した後、前記計算機に、前記IPSec処理を行える装置に割り振られたアドレス情報を通知することを特徴とする管理計算機。

【請求項１６】

管理計算機及び記憶装置システムと接続される計算機であって、

制御部、メモリ及び前記管理計算機及び前記記憶装置システムと接続されるネットワークと接続されるインターフェースとを有し、

前記管理計算機へ前記記憶装置システムにおける記憶領域の作成を前記インターフェースを介して要求し、前記制御部は、前記管理計算機から送信された複数のアドレスに関する情報を前記メモリに格納し、

前記複数のアドレスに関する情報から一つを選択して前記記憶装置システムが有する前記記憶領域にアクセスすることを特徴とする計算機。

【請求項１７】

前記計算機及び前記記憶装置システムは複数あることを特徴とする請求項１～１４記載の計算機システム。

【請求項１８】

計算機と、

前記計算機とネットワークを介して接続される記憶装置システムと、

前記計算機及び前記記憶装置システムと接続される第二の計算機とを有し、

前記第二の計算機は、前記記憶装置システムが前記ネットワークとの接続に用いる装置がIPSec処理を行えるかどうかに関する情報を有し、前記計算機のIPSec処理を行える前記装置に対応付けられた記憶領域の作成の要求に基づいて、前記要求に合致する前記記憶装置システムを前記情報に基づいて選択し、前記選択された記憶装置システムに対して前記計算機が使用する記憶領域を、前記記憶装置システムが有する前記装置のうち、IPSec処理を行える装置に対応付けて作成する指示を送信し、

前記記憶装置システムは、前記指示にしたがって、作成した記憶領域をIPSec処理を行える前記装置に対応付け、作成終了を前記第二の計算機へ通知し、

前記第二の計算機は、前記計算機に、IPSec処理を行える前記装置に割り当てられた前記ネットワークにおけるアドレスの情報を通知し、

前記計算機は、前記アドレスの情報に基づいて、前記記憶装置システムが有する前記記憶領域に、IPSec処理を行える前記装置を介してアクセスすることを特徴とする計算記シ

● 〃　ステム。

【書類名】明細書
【発明の名称】セキュリティレベルに応じて記憶領域を計算機に割り当てるシステム
【技術分野】
【０００１】
本発明は、インターネットプロトコル（IP）ネットワークを用いて複数の計算機や記憶装置システムを結合するストレージエリアネットワーク（以下「IP-SAN」）における記憶領域管理方法に関する。
【背景技術】
【０００２】
企業等でデータを効率よく管理するために、ストレージエリアネットワーク（SAN)が構築されることがある。SANとは複数の記憶装置システムと計算機とを結合するネットワークである。通常SAN内のデータ転送にはファイバチャネル・プロトコル（以下、このSANをFC-SANと言う）が用いられている。
【０００３】
一方、近年iSCSIを用いたSANであるIP-SANが注目されている。iSCSIとは、従来計算機と記憶装置システムとの間の通信に用いられていたSCSIコマンド及びそのコマンドに従って転送されるデータを、IPネットワーク経由で送受信するためのプロトコルである。ISCSIについては非特許文献１に詳細が開示されている。IP-SANは、FC-SANに比べ、すでにインフラストラクチャとして利用されている既存のLAN(Local Area Network)機器を活用することができる等の利点がある。
【０００４】
しかし、FC-SANとは異なり、IP-SANではインターネットや企業内LANなど、安全性が確保されていないネットワークを使用する場合がある。また、IPネットワークに対しての攻撃方法や攻撃プログラムが広く知れ渡っている。したがって、IP-SANでは、セキュリティに対する配慮が重要である。
【０００５】
SANでセキュリティを確保する方法として、計算機と記憶装置システムとの間でのアクセス制限や通信経路の暗号化が考えられる。計算機と記憶装置システムとの間でのアクセス制限技術として、スイッチやファブリックにおいて通信経路を分離するゾーニングや、ポート間においてエンドツウエンドのアクセス制限を行うＬＵＮマスキング(Logical Unit Number マスキング)がある。ここで、ＬＵＮマスキングの技術については、例えば特許文献１に開示されている。
【０００６】
IP-SANでは、計算機と記憶装置システムとの間の通信経路の暗号化方法としてIPSecを使用することができる。IPSecの詳細については非特許文献２に開示されている。IPSecは共通鍵を用いて通信の暗号化を行う技術である。IPSecでは、共通鍵の管理方式として非特許文献３により規定されるIKE(Internet Key Exchange)が採用されている。
【０００７】
【特許文献１】特開2001－265655号公報（第２－３項、第１－３図）
【非特許文献１】Julian Satran等著、「iSCSI」、２００３年１月１９日、IETF、＜URL: http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-20.txt＞
【非特許文献２】Stephen Kent、Randall Atkinson著、「Security Architecture for IP」、１９９８年１１月、IETF、＜URL: http://www.ietf.org/rfc/rfc2401.txt＞
【非特許文献３】Dan Harkins、Dave Carrel著、「The Internet Key Exchange (IKE)」、１９９８年１１月、IETF、＜URL: http://www.ietf.org/rfc/rfc2409.txt＞
【発明の開示】
【発明が解決しようとする課題】
【０００８】
IP-SANに接続される装置がすべて上述したセキュリティ確保のための機能を有する訳ではない。例えば、IP-SANに接続される装置には、IPSecが実装されているものとされてい

ないものがある。又、計算機と記憶装置システムとの間の全ての通信においてセキュリティを確保する必要が無い場合もある。

【０００９】

このような場合、システム管理者はシステムを構築する際、ネットワークに接続された機器のセキュリティ確保のための機能の有無やシステム内の各部におけるセキュリティレベルを逐次考慮しながら、ネットワークに接続された計算機に、ネットワークに接続された記憶装置システムやその記憶装置システムが有する記憶領域を割り当てる必要がある。これはシステム管理者に過大な負荷がかかる。又、管理者が設定した場合、計算機の使用者が自由にその記憶領域の割当ての設定を変更することが難しい。あるいは、計算機と記憶装置システムとの間の通信で不必要にセキュリティレベルが高い設定がなされ、システムの資源を無駄に使用してしまう。

【課題を解決するための手段】

【００１０】

本発明は上記の問題を解決するため、以下の構成を有する。具体的には、ネットワークに接続される計算機や記憶装置システムの情報を管理する計算機（以下「管理計算機」とも言う）を有するシステムとする。そして、管理計算機は、計算機の要求に従って所定の条件を有する記憶装置システムを選択し、その記憶装置システムに対して記憶領域の作成を指示する。指示を受けた記憶装置システムは、指示された条件に従って記憶領域を作成し、管理計算機に作成終了を通知する。

【００１１】

通知を受けた管理計算機は、作成された記憶領域を使用するための情報（例えば記憶装置システムが有するポートに振られたネットワークにおけるアドレス等）を計算機に通知する。計算機は通知された情報に基づいて、作成された記憶領域を使用する。

【００１２】

ここで、管理計算機が管理する記憶装置システム等の情報とは、セキュリティレベルに関する情報である。又、計算機の要求にはセキュリティレベルに関する要求が含まれていても良い。この場合、管理計算機は、計算機から要求されたセキュリティレベルに合致する記憶装置システムを自身が管理する情報から検索し、その記憶装置システムに対し、記憶領域の作成を指示する。

【００１３】

尚、ここでセキュリティレベルとは、各装置においてデータ送受信の暗号化処理が可能かどうかを示す情報でも良い。

【００１４】

本発明の他の構成については、実施例等の記載により明らかにされる。

【発明を実施するための最良の形態】

【００１５】

図１は、本発明の第一の実施形態におけるシステム構成例を示す図である。システムは、計算機（以下「サーバ」とも言う）１０１、記憶装置システム１０２及び管理計算機（以下「管理サーバ」とも言う）１０３を有する。サーバと記憶装置システムとは、IPネットワーク１０４で相互に接続されている。また、サーバ、記憶装置システム及び管理サーバは管理用ネットワーク１０５により相互に接続される。

【００１６】

なお、図１に示したシステム構成例ではIPネットワーク１０４と管理用ネットワーク１０５をそれぞれ独立したネットワークとして構成しているが、それらを一つのネットワークで共有する構成にしても良い。また、IPネットワーク１０４に接続されるサーバ１０１と記憶装置システム１０２の数は任意である。

【００１７】

サーバ１０１は、IPネットワーク１０４を介して記憶装置システム１０２との間でデータの送受信を行う。IPネットワーク１０４はIPパケットを転送可能なネットワークである。具体的にIPネットワークには、イーサネット（登録商標）により構築されたLANやWAN(W

ＩＤe Area Network)、通信事業者により提供される広域IP通信網、専用線等がある。

【００１８】

管理サーバ１０３は、管理用ネットワーク１０５を介してサーバ１０１や記憶装置システム１０２との間で管理情報の送受信を行う。

【００１９】

サーバ１０１は一般的な計算機であり、プロセッサ（以下「ＣＰＵ」とも言う）１０６、メモリ１０７及びホストバスアダプタ（以下「ＨＢＡ」とも言う）１０８を有する。ＣＰＵ１０６、メモリ１０７及びＨＢＡ１０８は、バス１０９を介して相互に接続される。メモリには、パス管理プログラム１１０、パス情報テーブル１１１及びパスワード管理テーブル１１２が格納される。尚、これらのプログラムは、可搬記憶媒体やネットワークを介してサーバ１０１のメモリ１０７等に格納される。

【００２０】

プロセッサ１０６は、パス管理プログラム１１０を実行することで、パス情報テーブル１１１に格納されているサーバと記憶装置システムとの間の経路情報を元に、IPネットワーク１０４を介したサーバ１０１と記憶装置システム１０２との間のデータ通信経路を決定する。またプロセッサ１０６は、管理者、ユーザ、他のプログラム等からの情報を元に、データ通信経路の決定や変更を行う。

【００２１】

パス情報テーブル１１１には、サーバ１０１が、IPネットワーク１０４に接続される記憶装置システム１０２へアクセスするために必要な経路情報と、その経路が持つ特性情報（IPSecによる暗号化機能の有無等）が格納される。

【００２２】

IPSecを用いてサーバ１０１と記憶装置システムとの間でデータを暗号化して通信する際には、暗号化に必要な鍵を、通信を行うサーバ１０１と記憶装置システム１０２とに設定する必要がある。鍵を設定する鍵管理方法には手動管理方式と自動管理方式がある。ただし、iSCSIの規約では、手動管理方式による鍵管理が禁止されている。また、iSCSI規約では、自動管理方式としてIKE鍵管理プロトコルを実装しなくてはならないと規定している。IKEで鍵交換を行う際、サーバ１０１と記憶装置システムとの間で相互の認証処理が行われる。パスワード管理テーブル１１２には、IKEでの認証時に必要となる、装置自身のパスワードが格納される。尚、iSCSI規約に従わなくても良い状況で本発明を使用する場合には、手動管理方式で鍵を設定しても良いし、IKE以外のプロトコルの自動管理方式を採用しても良い。

【００２３】

ＨＢＡ１０８は、サーバ１０１とIPネットワーク１０４とを接続するために用いられる接続機器である。ＨＢＡ１０８は、インターフェースチップ（以下「ＩＦチップとも言う」）１１３、IPネットワーク１０４へ接続するための物理ポート１１５及びIPSec処理部１２７を有する。サーバ１０１とIPネットワーク１０４との間で転送されるデータは、すべてポート１１５を介して転送される。

【００２４】

ＩＦチップ１１３は、IPネットワーク１０４へ送受信するパケットの処理（SCSIコマンドのカプセル化等）及び物理ポート１１５とサーバ１０１のメモリ１０７等との間のDMA(Direct Memory Access)転送を制御する回路である。

【００２５】

IPSec処理部１２７は、通信されるデータの暗号化、復号化、装置間の鍵交換及び認証に関する処理等を行うプロセッサである。認証を行う際には、IPSec処理部１２７は、メモリ１０７に格納されたパスワード管理テーブル１１２を検索し、通信相手との認証に必要なパスワードを入手する。

【００２６】

尚、本実施形態では、ＨＢＡ１０８として、IPSecによる暗号化通信に必要な処理を行えるＨＢＡを仮定した。しかしながら、サーバ１０１は、実際にはIPSec処理が行えない

ＨＢＡ１０８を有する場合もある。以下、これらのＨＢＡを区別する場合、IPSecの処理を行えるＨＢＡ１０８をＨＢＡ１０８ａとし、IPSecの処理を行えないＨＢＡ１０８をＨＢＡ１０８ｂとする。

【００２７】

記憶装置システム１０２は、ホストアダプタ１２０ａ、ホストアダプタ１２０ｂ、ＣＰＵ１１６、ディスクアダプタ１１７、メモリ１１９、キャッシュメモリ１１８、ディスクドライブ群１２１を有する。ホストアダプタ１２０ａ、ホストアダプタ１２０ｂ、ＣＰＵ１１６、ディスクアダプタ１１７、メモリ１１９及びキャッシュメモリ１１８は、バス１２２を介して相互に接続される。バス１２２の代わりにスイッチが用いられても良い。ディスクアダプタ１１７は、ディスクドライブ群１２１とバス１２２とを相互に接続する。メモリ１１９には、ボリューム情報テーブル１２３及びパスワード管理テーブル１２４が格納される。

【００２８】

ＣＰＵ１１６は、バス１２２を介してメモリ１１９へアクセスし、メモリ１１９へ格納されたプログラムを実行する。ディスクアダプタ１１７は、ＣＰＵ１１６からディスクドライブ群１２１へのアクセスの制御を行う。キャッシュメモリ１１８には、サーバ１０１へ転送されるデータあるいはサーバ１０１から転送されてきたデータが一時的に格納される。

【００２９】

ディスクドライブ群１２１は、１つ又は複数のディスクドライブを有する。尚、ディスクドライブ群１２１は、ディスクドライブのような不揮発性記憶媒体の代わりに、フラッシュメモリカード等の揮発性の記憶媒体を複数有していても良い。個々のディスクドライブは物理的な記憶領域を有する。記憶装置システム１０２は、個々のディスクドライブが有する物理的な記憶領域から、論理的な記憶領域（以下「物理ボリューム」という）を作成する。この物理ボリュームは、記憶装置システム１０２が、自身が有する記憶領域を１つの論理的な記憶装置として扱う単位となる。尚、この物理ボリュームを構成するディスクドライブ群がＲＡＩＤ構成であっても良い。

【００３０】

さらに記憶装置システム１０２は、１又は複数の物理ボリュームから、ボリュームを作成する。ボリュームは、サーバ１０１に対して提供される論理的な記憶領域の一つの単位であり、例えば、SCSI規格で使用される論理ユニット(Logical Unit：LU)に相当する。

【００３１】

ホストアダプタ１２０は、IPネットワーク１０４と接続される物理ポート１２５を有する。また、ホストアダプタ１２０ａは、IPSecによる暗号化通信に必要な処理を行うためのIPSec処理部１２７を有する。本実施形態では、記憶装置システム１０２がIPSecによる暗号化通信処理を行うホストアダプタ１２０ａとIPSecによる暗号化通信処理を行わないホストアダプタ１２０ｂを一つづつ有する構成としたが、記憶装置システム１０２が有するホストアダプタ１２０ａ、ｂの数は任意である。記憶装置システム１０２は、ホストアダプタ１２０ａのみ又はｂのみを有していても良い。

【００３２】

ボリューム情報テーブル１２３には、物理ボリュームとボリュームとの対応関係を示す情報が格納される。具体的には、ある物理ボリュームに対応するボリュームの番号（以下論理ユニット番号（ＬＵＮ）と言う）、ボリュームの容量、ボリュームに割り当てられたポート１１５のＩＤ（アドレス等）情報が保持される。記憶装置システム１０２は、新しいボリュームを作成するたびにボリューム情報テーブル１２３の内容を更新する。

パスワード管理テーブル１２４には、記憶装置システム１０２のホストアダプタ１２０ａがIPSec処理をする際のIKEでの認証時に必要とするパスワードが格納される。

【００３３】

管理サーバ１０３は、一般的な計算機であり、プロセッサ（以下「ＣＰＵ」とも言う）１２８、メモリ１２９、及びネットワーク接続部１３０を有する。ＣＰＵ１２８、メモリ

１２９、及びネットワーク接続部１３０は、バス１３１により相互に接続される。メモリ１２９には、ネットワーク管理プログラム１３２及び構成データベース１３３が格納される。

【００３４】

構成データベース１３３は、ポート情報テーブル１３４及びストレージ容量管理テーブル１３５を有する。

ポート情報テーブル１３４には、管理サーバ１０３がIPネットワーク１０４に接続されている物理ポートを管理するための情報が登録される。具体的には、ある物理ポートに対し、その物理ポートを持つ装置を一意に識別する装置ＩＤ、その物理ポートへ他の装置がアクセスするためのアドレス、その物理ポートを保持するＨＢＡやホストアダプタがIPSec処理を実行可能か否かの情報が保持される。

【００３５】

ストレージ容量管理テーブル１３５には、管理サーバ１０３がIPネットワーク１０４に接続されている記憶装置システム１０２の記憶容量を管理するための情報が登録される。具体的には、IPネットワーク１０４に接続される個々の記憶装置システム１０２が有する記憶領域のうち、まだ使用されていない記憶領域の容量（以下「空き容量」）及び既に使用されている記憶領域の容量（以下「使用済み領域の容量」又は「使用容量」）の情報が、記憶装置システム１０２毎にストレージ容量管理テーブル１３５に登録される。

【００３６】

管理サーバ１０３のプロセッサ１２８は、ネットワーク管理プログラム１３２を実行して、管理用ネットワーク１０５を介し、サーバ１０１や記憶装置システム１０２がそれぞれ持つ物理ポートの情報、ストレージの空き容量や使用済み領域の容量の情報を収集する。そして、管理サーバ１０３は、収集した情報に基づいて、ポート情報テーブル１３４とストレージ容量管理テーブル１３５を作成したり、更新したりする。

【００３７】

また、管理サーバ１０３は、サーバ１０１やシステム管理者等からのボリューム作成要求に基づいて、ポート情報テーブル１３４とストレージ容量管理テーブル１３５の内容を検索し、条件にあったボリュームの作成要求を記憶装置システム１０２に対して発行する。更に、ボリューム作成の完了報告を記憶装置システム１０２から受領した管理サーバ１０３は、ボリューム作成が完了したことを、ボリューム作成要求を発行したサーバ１０１や管理者等へ通知する。さらに、管理サーバ１０３は、ＩＫＥを行う際の認証に必要なパスワードを収集し、サーバ１０１及び記憶装置システム１０２へ、新たに入力されたパスワードをパスワード管理テーブル１１２、１１７へ登録する命令を発行する。

【００３８】

以下、各機器が有する各テーブルの内容について説明する。なお、本実施形態では情報はテーブルの形態で管理されているが、情報の管理の仕方はテーブルに限られない。

図２は、ポート情報テーブル１３４の構成例を示す図である。ポート情報テーブル１３４は、IPネットワーク１０４へ接続されている各物理ポート１１５、１２５（以下まとめて「物理ポート１１５等」又は単に「物理ポート」）の特性の情報を保持するテーブルである。

【００３９】

ポート情報テーブル１３４は、IPネットワーク１０４に接続される物理ポート１１５等数分のエントリを有する。１つのエントリは、そのエントリに対応する物理ポート１１５等を有する装置の識別子である装置ＩＤを登録するフィールド２０１、対応する物理ポート１１５等へ割り当てられているSCSIオブジェクトのオブジェクトＩＤを登録するフィールド２０２、対応する物理ポート１１５等へ割り当てられているIPアドレスを登録するフィールド２０３、対応する物理ポート１１５等を保持する装置がサーバ１０１であるか記憶装置システム１０２であるかを区分する情報であるノード種別が登録されるフィールド２０４、対応する物理ポート１１５等を持つＨＢＡ１０８やホストアダプタ１２０がIPSec処理部を持つか否かを示す情報が登録されるフィールド２０５、認証ＩＤが登録される

フィールド２０６及びパスワードを登録するフィールド２０７を有する。

【００４０】

ここで物理ポートへのSCSIオブジェクトの割当てとは、サーバ１０１がSCSIオブジェクトを使用するときに使用する物理ポートを決定することを指す。従って、サーバ１０１は、他の物理ポートを用いてSCSIオブジェクトを利用することは出来ない。

【００４１】

オブジェクトＩＤとは、ＳＡＭ（SCSI Architecture Model）にて規定されるSCSIオブジェクトの識別子である。ここでSCSIオブジェクトとは、SCSIコマンドを発行する装置（論理的でも物理的でも良い。以下「SCSIイニシエータ」）と、SCSIコマンドを受信する装置（論理的でも物理的でも良い。以下「SCSIターゲット」）の総称である。オブジェクトＩＤは、iSCSIではiSCSIネーム、FCではWWNに相当する。IPネットワーク１０４に接続する装置は１つ以上のSCSIオブジェクトを持つことが可能である。例えば図２に示す例では、装置ＩＤがStorage1である記憶装置システム１０２はiqn.2003-03.com.example:storage1及びiqn.2003-04.com.example:storage１の２つのSCSIオブジェクト（ここではSCSIターゲット）を保持している。

【００４２】

また、物理ポート１１５等がSCSIオブジェクトへ割り当てられていない場合、フィールド２０２は空欄になる。例えば、図２に示す例において、装置ＩＤがStorage2である記憶装置システム１０２の、割り当てIPアドレスが10.10.10.204である物理ポートは、フィールド２０２が空欄になっている。これは、この物理ポートがSCSIオブジェクトへ割り当てられていないことを示している。

【００４３】

認証ＩＤは、IPSecの暗号化処理におけるＩＫＥ認証において、鍵交換を行う端末を特定するＩＤである。認証ＩＤは、IPSecを使用可能な物理ポート毎に割り当てられる。認証ＩＤは、例えば物理ポートに割り当てられているIPアドレス、IPアドレスとネットワークマスクの組又は装置ＩＤなどの名前が使用されても良い。

【００４４】

パスワードは、ＩＫＥ認証に使用されるパスワードであり、認証ＩＤ同様、IPSecを使用可能な物理ポート毎に割り当てられる。フィールド２０７には、パスワード設定方式としてPre-Shared方式を使用している場合にはパスワード文字列が、デジタル署名を使用している場合には認証局から発行されたデジタル署名がパスワードとして格納される。例えば、図２に示す例において、Host１が持つIPアドレス10.10.10.101の物理ポート１１５については、認証ＩＤとしてIPアドレス、パスワード設定方法としてPre-Shared方式を用いることで、フィールド２０６へは10.10.10.101、フィールド２０７へはパスワード文字列aaaaaaという値が格納されている。

【００４５】

ポート情報テーブル１３４は管理サーバ１０３により管理される。管理サーバ１０３は、システムに新しい物理ポート１１５等が追加されたり、新たに物理ポート１１５等へボリュームが割り当てられたり、パスワードの設定が行われる度にポート情報テーブル１３４を更新する。

【００４６】

図３は、ストレージ容量管理テーブル１３５の構成例を示す図である。ストレージ容量管理テーブル１３５は、IPネットワーク１０４へ接続している記憶装置システム１０２が有する記憶領域の使用状況の情報を保持するテーブルである。

ストレージ容量管理テーブル１３５は、IPネットワーク１０４に接続されている記憶装置システム１０２の数分のエントリを有する。各エントリは、対応する記憶装置システム１０２の識別子である装置ＩＤを登録するフィールド３０１、対応する記憶装置システム１０２の空き容量の情報を登録するフィールド３０２及び対応する記憶装置システム１０２の使用容量の情報を登録するフィールド３０３を有する。

【００４７】

空き容量は、記憶装置システム１０２において、ディスクドライブ群１２１が有する記憶領域のうち、物理ボリュームが作成されていない記憶領域の記憶容量を示す情報である。また、使用容量はディスクドライブ群１２１が有する記憶領域のうち、すでに物理ボリュームとして使用されている記憶領域の記憶容量を示している。

例えば図３に示す例では、Storage 1が有する記憶領域のうち、空き容量は１０Ｔバイトであり、使用容量は５Ｔバイトである。ストレージ容量管理テーブル１３５はネットワーク管理プログラム１３２により管理される。ネットワーク管理プログラム１３２は、IPネットワーク１０４へ接続している記憶装置システムへ新しい物理ボリュームが作成される度（あるいは削除される度）にストレージ容量管理テーブル１３５の内容を更新する。

【００４８】

図４は、サーバ１０１が保持するパス情報テーブル１１１の構成例を示す図である。パス情報テーブル１１１は、サーバ１０１がIPネットワーク１０４を介して使用する仮想的な記憶装置（以下「ディスクデバイス」）の名前と、サーバ１０１がディスクデバイスへアクセスするための情報を保持するテーブルである。パス情報テーブル１１１は、サーバ１０１が使用するディスクデバイスの数分のエントリを有する。

【００４９】

個々のエントリは、対応するディスクデバイスに対してサーバ１０１で付与された名前であるデバイス名を登録するフィールド４０１、対応するディスクデバイスを含むSCSIオブジェクトのオブジェクトＩＤを登録するフィールド４０２、ディスクデバイスに対応するボリュームのＬＵＮを登録するフィールド４０３、対応するディスクデバイスを含むSCSIオブジェクトに割り振られた物理ポートのIPアドレスを登録するフィールド４０４及び対応するディスクデバイスを含むSCSIオブジェクトに割り振られた物理ポートのＴＣＰポート番号が登録されるフィールド４０５を有する。

【００５０】

ここで、ディスクデバイスとは、サーバ１０１で実行されるオペレーティングシステム（「OS」）等のプログラムにおいて扱われる記憶領域の単位である。ディスクデバイスは一つ又は複数のボリュームから構成される。本実施形態では、デバイス名の例として、例えば、図４に示すように「/dev/had」等の名前が用いられる。パス情報テーブル１１１の内容は、システムの管理者が手動で設定しても良いし、ホスト１０１上のOSやパス管理プログラム１１０が任意にデバイス名等を設定しても良い。

【００５１】

尚、１つのSCSIオブジェクト（例えばSCSIターゲット）が複数のディスクデバイスを有していても良く、逆に複数のSCSIオブジェクトから一つのディスクデバイスが構成されていても良い。又、SCSIオブジェクトは、１つ又は複数のボリュームから構成される。

【００５２】

図５は、記憶装置システム１０２が保持するボリューム情報テーブル１２３の構成例を示す図である。ボリューム情報テーブル１２３は、各記憶装置システム１０２で作成された物理ボリュームの特性に関する情報を保持するテーブルである。ボリューム情報テーブル１２３は、記憶装置システム１０２が有する物理ボリュームの数分のエントリを有する。各エントリは、対応する物理ボリュームの識別子である物理ボリューム番号を登録するフィールド５０１、物理ボリュームに対応するボリュームのＬＵＮを登録するフィールド５０２、対応する物理ボリュームの容量を登録するフィールド５０３、対応する物理ボリュームを含むSCSIオブジェクトのオブジェクトＩＤを登録するフィールド５０６、対応する物理ボリュームを含むSCSIオブジェクトに対応付けられた物理ポートに割り振られたIPアドレスを登録するフィールド５０４、対応する物理ボリュームを含むSCSIオブジェクトとＴＣＰコネクションを確立するために使用するＴＣＰポートのポート番号を登録するフィールド５０５及び物理ボリュームに対応する物理ポートを有するＨＢＡ等がIPSec処理部を持つか否かを示す情報を登録するフィールド５０７を有する。

【００５３】

ボリューム情報テーブル１２３は、記憶装置システム１０２により管理される。記憶装

置システム１０２は、物理ボリュームを作成し、その物理ボリュームからボリュームを作成するごとに作成したボリュームの特性をボリューム情報テーブル１２３へ登録する。

【００５４】

図６は、IPネットワーク１０４へ接続している装置が保持するパスワード管理テーブル１２４の構成例を示す図である。パスワード管理テーブル１２４は、そのテーブルを保持している装置が暗号化通信を行う相手の数分のエントリを有する。パスワード管理テーブルの各エントリは、IPSecを用いた暗号化通信を行う通信相手に対する認証ＩＤの情報を登録するフィールド６０１及び暗号化通信の際にＩＫＥでの認証に用いるパスワードを登録するフィールド６０２とを有する。

パスワード管理テーブル１１２は、パスワードの登録が行われる度に更新される。

【００５５】

本実施形態では、サーバ１０１の使用者（あるいは管理者）が記憶装置システム１０２の記憶領域を新たに使用したい場合、使用者は管理サーバ１０３に対してボリュームの作成要求を発行する。この際、使用者は、作成したいボリュームの特性（ここではセキュリティレベル）についての要求もボリューム作成の要求に含める。ボリュームの作成要求を受領した管理サーバ１０３は、使用者の要求（ここでは記憶容量とセキュリティレベル）に応じたボリュームが作成可能な記憶装置システム１０２をポート情報テーブル１３４及びストレージ容量管理テーブル１３５から検索する。

【００５６】

検索の結果、使用者の要求に合致する記憶装置システム１０２が検索された場合、管理サーバ１０３は、検索された記憶装置システム１０２に対して、使用者が要求するボリュームの作成を指示する。特に、高いセキュリティレベル（ここではIPSecによる暗号化通信）が使用者から要求される場合には、管理サーバ１０３は、記憶装置システム１０２に対して、作成したボリュームをIPSec処理部を有するＨＢＡ等が有する物理ポート（以下「IPSec機能を有する物理ポート」とも言う）に割り付けるように指示する。

【００５７】

その後、記憶装置システム１０２からボリューム作成の完了を受信した管理サーバ１０３は、ボリューム作成の完了とそのボリュームを使用するための情報（ボリュームと対応付けられたIPアドレス等）を使用者（サーバ１０１や管理者）に送信する。ボリューム作成完了の通知を受けた使用者は、受信した情報を用いて、作成されたボリュームを使用（ボリュームを用いたディスクデバイスの作成等）する。サーバ１０１がセキュリティが確保されたボリュームに対して通信を行う際は、サーバ１０１は、IPSecのプロトコルにのっとり、まず認証ＩＤ及びパスワードを、ボリュームを有する記憶装置システム１０２に送信する。記憶装置システム１０２は、送信された認証ＩＤ及びパスワードを用いて、サーバ１０１の認証を行う。サーバ１０１が記憶装置システム１０２に認証された後、サーバ１０１は、ボリュームに格納するデータを暗号化して記憶装置システム１０２へ送信する。

【００５８】

以下、本実施形態の処理手順の詳細について説明する。

図７は、本実施形態におけるボリューム割り当て処理全体の手順を示す図である。まず、管理サーバ１０３は、サーバ１０１や管理者からのボリューム作成要求を受信するまで構成情報管理処理を行っている（ステップ７０１）。管理サーバ１０３は、サーバ１０１や管理者からボリューム作成要求を受信する（ステップ７０２）と、ボリューム作成と割り当て処理７０３を実行する。この処理により、サーバ１０１が新しいボリュームを使用することが出来る。ステップ７０１及び７０３での処理の詳細は後述する。

【００５９】

図８は、管理サーバ１０３が実行する構成情報管理処理の手順を示す図である。構成情報管理処理では、管理サーバ１０３が、IPネットワーク１０４への新しい物理ポート１１５等の追加、追加された物理ポートのIPSec機能の有無、記憶装置システム１０２の容量追加等を検知し、各種テーブルの内容を更新する。

【００６０】
管理サーバ１０３は、サーバ１０１等からボリューム作成の指示を受けつけていない場合は、常に（又は一定の間隔、任意の時間に）IPネットワーク１０４に新しい物理ポート１１５等が接続されたかどうかを探索している。具体的には、システムの管理者が手動で物理ポートの追加を管理サーバ１０３に通知しても良いし、管理サーバ１０３が管理用ネットワーク１０５を通じてIPネットワーク１０４に接続される装置の構成情報を定期的に収集しても良い。

【００６１】
IPネットワーク１０４に接続される装置の構成情報を定期的に収集する方法の一例としては、管理サーバ１０３がSNMP(Simple Network Management Protocol)を用いてIPネットワーク１０４に接続される装置からMIB(Management Information Base)を収集する方法がある。また、そのほかに、管理用ネットワーク１０５にiSNS（Internet Storage Name Service）サーバが接続している場合は、管理サーバ１０３が、iSNSサーバが発行するSCN(State Change Notification)を管理用ネットワーク１０５経由で検知する方法もある。ここで、iSNSとは、Internet draftである「Internet Storage Name Service」にて規定される公知技術であり、IP-SANデバイス及びFC-SANデバイスを発見、識別、管理する機能を提供できる（参考　＜URL：http://www.ietf.org/internet-drafts/draft-ietf-ips-isns-21.txt＞）（ステップ８０１）。

【００６２】
ネットワーク１０４に新たな物理ポートが追加されたことを検出した場合、管理サーバ１０３は、新しく追加された物理ポートのIPSec機能の有無、物理ポートをもつ装置の装置ＩＤ及びその装置のノード種別を収集する。そして、管理サーバ１０３は、収集した情報をポート情報テーブル１３４へ登録する。情報の収集方法は、例えばシステムの管理者が手動で管理サーバ１０３へ入力する方法でも良いし、管理サーバ１０３がMIB等を用いて追加された物理ポートを有する装置から自動的に収集しても良い（ステップ８０２）。

【００６３】
その後、管理サーバ１０３は、新しく追加された物理ポートへIPアドレスとオブジェクトＩＤを割り当てる。ただし、オブジェクトＩＤに関しては、このステップで割り当てなくとも良い。この場合、オブジェクトＩＤは管理サーバ１０３及び記憶装置システム１０２が実行するボリューム作成と割り当て処理の際に物理ポートに割り当てられる。IPアドレスの割り当て方法は、システムの管理者が手動で管理サーバ１０３へIPアドレスを入力しても良いし、管理サーバ１０３がDHCP（Dynamic Host Configuration Protocol）等のプログラムを利用してIPアドレスを自動的に割り当てても良い。

【００６４】
オブジェクトＩＤの割り当て方法は、システムの管理者が手動で管理サーバ１０３へオブジェクトＩＤを入力しても良いし、新しく追加された物理ポートを持つ装置がポートに自動的にオブジェクトＩＤを割り当てても良い。管理サーバ１０３は、割り当てられたIPアドレスとオブジェクトＩＤをシステムの管理者による通知やMIB等の情報により検知し、ポート情報テーブル１３４へ登録する。オブジェクトＩＤの割り当てを行わなかった場合には、図２において、装置ＩＤがStorage2である記憶装置システム１０２の、割り当てIPアドレスが10.10.10.204である物理ポートのように、フィールド２０２が空欄となる（ステップ８０３）。

【００６５】
その後、管理サーバ１０３は、ステップ８０２で収集した情報に基づいて、追加された物理ポートがIPSecの機能を有するかどうか（具体的には、追加された物理ポートを有するＨＢＡ等がIPSec処理部を有するかどうか）を判定する（ステップ８０４）。
追加された物理ポートがIPSec機能を有する場合、管理サーバ１０３は、追加された新しい物理ポートがＩＫＥ認証で用いる認証ＩＤとパスワードの設定を行う。管理サーバ１０３は、システムの管理者へ認証ＩＤとパスワードを設定するよう通知する。管理者等は、管理サーバ１０３が有する入力インターフェースを介して新しい物理ポートについての

認証ＩＤとパスワードの情報を入力する。管理サーバ１０３は、入力された認証ＩＤとパスワードを、ポート情報テーブル１３４に登録する（ステップ８０５）。

【００６６】

ステップ８０１で新しい物理ポートを発見しなかった場合、ステップ８０４で新しく追加された物理ポートがIPSec機能を有さなかった場合又はステップ８０５の処理の後、管理サーバ１０３は、IPネットワークに接続される記憶装置システム１０２の記憶容量の変化や新しく接続された物理ポートを有する装置が記憶装置システム１０２であるかどうかを判定する。管理サーバ１０３が新しい記憶装置システム１０２の追加を検出する方法や既存の記憶装置システム１０２の記憶容量の記憶容量の変化を検出する方法は、IPネットワーク１０４への物理ポートの接続の検出方法と同様である。すなわちシステムの管理者の手動設定やMIB等の構成情報の定期的な収集である（ステップ８０６）。

【００６７】

記憶装置システム１０２の追加や既存の記憶装置システム１０２の記憶容量の変化を検出した管理サーバ１０３は、新しく追加された記憶装置システム１０２（又は変更があった記憶装置システム１０２）の記憶容量をストレージ容量管理テーブル１３５へ登録する。管理サーバ１０３が記憶装置システム１０２の記憶容量の情報を収集する方法も、上述の物理ポートの検出方法等と同じ方法が考えられる（ステップ８０７）。

【００６８】

ステップ８０６で新しい記憶装置システム１０２の追加や記憶装置システム１０２の容量変化を検出しなかった場合又はステップ８０７の実行後、管理サーバ１０３は、ネットワーク１０４から物理ポートが削除（具体的にはネットワーク１０４から物理ポートが外されること）されたかを判定する。管理サーバ１０３が物理ポートの削除を検出する方法は、削除されたポートのIPアドレスを、システムの管理者による通知や定期的に収集したMIB等の情報より検知する方法が考えられる（ステップ８０８）。

【００６９】

ネットワーク１０４から削除された物理ポートのIPアドレスを検知した管理サーバ１０３は、ポート情報テーブル１３４のフィールド３０３を検索することで削除された物理ポートの情報を特定し、同情報をポート情報テーブル１３４から削除する（ステップ８０９）。

【００７０】

図９及び図１０は、管理サーバ１０３及び記憶装置システム１０２が実行するボリューム作成と割り当て処理の手順を示す図である。ボリューム作成と割り当て処理は、サーバ１０１や管理者からボリュームの作成要求を受けた際に実行される。サーバ１０１や管理者から管理サーバ１０３へ送信されるボリューム作成要求には、作成されるボリュームに必要な記憶容量、作成されるボリュームへのアクセスのセキュリティレベル、例えばボリュームへアクセスする際にIPSecによる暗号化が必要か否かの情報が含まれる。

【００７１】

最初に管理サーバ１０３は、ボリューム作成要求に含まれるボリュームへのアクセスについてのセキュリティレベルの情報に基づいて、作成が要求されたボリュームへのアクセスについてIPSecによる暗号化通信が必要か否かの判定を行う（ステップ９０１）。

作成が要求されるボリュームへのアクセスについてIPSecに基づく暗号化通信が不要であると判断した場合、管理サーバ１０３は、ポート情報テーブル１３４のフィールド３０５を検索し、IPSec機能を持たない物理ポートを特定する。そして、管理サーバ１０３は、特定した物理ポートのIPアドレス及び物理ポートを保持する記憶装置システム１０２の装置ＩＤを特定する。次に管理サーバ１０３は、特定した装置ＩＤでストレージ容量管理テーブル１３５を検索し、特定した装置ＩＤを有する記憶装置システム１０２の空き容量を確認する。そして管理サーバ１０３は、特定した装置ＩＤを有する記憶装置システム１０２の中から、作成が要求されたボリュームの記憶容量以上の空き容量を有する記憶装置システム１０２を特定する（ステップ９０２）。

【００７２】

次に管理サーバ１０３は、ステップ９０２で特定した記憶装置システム１０２へ、サーバや管理者から要求された記憶容量を有するボリュームの作成を指示する命令を発行する。

ボリューム作成の命令を受信した記憶装置システム１０２は、要求された記憶容量のボリュームを作成する。ボリューム作成を終了した記憶装置システム１０２は、ボリューム作成の終了を管理サーバ１０３へ送信する。

【００７３】

ボリューム作成終了の通知を受信した管理サーバ１０３は、ボリュームを作成した記憶装置システム１０２に対して、作成したボリュームをIPSec機能を持たない物理ポートへ割り当てることを指示する命令を発行する。この命令には、管理サーバ１０３がステップ９０２で収集した、特定された記憶装置システム１０２が有するIPSec機能を持たない物理ポートに割り振られたIPアドレスの情報が含まれる。

【００７４】

管理サーバ１０３からポート割り当て命令を受けた記憶装置システム１０２は、作成したボリュームを指定された物理ポートへ割り当てる。

【００７５】

続いて記憶装置システム１０２は、作成したボリュームへTCPコネクションを確立する際に使用するＴＣＰポート番号を決定する。ＴＣＰポート番号を決定する方法は、記憶装置システム１０２が自動的に決定しても良いし、ボリューム作成要求を発行したサーバ１０１や管理者へＴＣＰポート番号を決めるように促しても良い。また、管理サーバ１０３がポート割り当て命令を発行する前に、管理サーバ１０３が自動的にＴＣＰポート番号を決定する、或いは、管理サーバ１０３がボリューム作成要求を発行したサーバ１０１や管理者へＴＣＰポート番号を決定するよう促し、決定したＴＣＰポート番号をポート割り当て命令に含める方法でも良い。割当てを終了した記憶装置システム１０２は、その結果を管理サーバ１０３へ通知する（ステップ９０３）。

【００７６】

上記の例では、管理サーバ１０３からボリューム作成命令とポート割り当て命令を別々に発行しているが、それらを一つにまとめた命令を発行する構成も考えられる。そのような構成におけるステップ９０３の動作手順を以下に説明する。

【００７７】

管理サーバ１０３は、ステップ９０２で特定した記憶装置システム１０２へボリューム作成・ポート割り当て命令を発行する。この命令は、サーバや管理者から発行された記憶容量を有するボリュームの作成を指示する命令及び作成したボリュームをIPSec機能を有しない物理ポート１２５へ割り当てることを指示する命令を含む。また、この命令には、管理サーバ１０３がステップ９０２で収集した、特定された記憶装置システム１０２が有するIPSec機能を有しない物理ポートに割り振られたIPアドレスの情報が含まれる。さらに、作成したボリュームへＴＣＰコネクションを確立する際に使用するＴＣＰポート番号を含めても良い。

【００７８】

ボリューム作成・ポート割り当て命令を受信した記憶装置システム１０２は、要求された記憶容量のボリュームを作成する。ボリューム作成に失敗した場合、記憶装置システム１０２は、管理サーバ１０３へエラー情報を発行する。ボリューム作成に成功した場合、記憶装置システム１０２は、作成したボリュームを指定された物理ポート１２５へ割り当てる。割り当てを完了した記憶装置システム１０２は、その結果を管理サーバ１０３へ通知する。

【００７９】

ステップ９０２の処理で要求されたボリュームを作成可能な記憶装置システム１０２がシステム上に存在しなかったり、記憶装置システム１０２の故障などの理由によりステップ９０３で行われる処理が失敗した場合、管理サーバ１０３は、ボリューム作成要求を発行したサーバ１０１や管理者へエラー情報を通知し、ボリューム作成と割り当て処理を終

了する（ステップ９０６）。

【００８０】

ステップ９０２及び９０３の処理が成功した場合、管理サーバ１０３は、ストレージ容量管理テーブル１３５及びボリューム情報テーブル１２３の内容の更新を行う。具体的には、管理サーバ１０３は、ストレージ容量管理テーブル１３５の内、ステップ９０３でボリュームを作成した記憶装置システム１０２の空き容量を作成したボリュームの容量分減らし、使用容量を作成したボリュームの容量分増加させる。

【００８１】

また管理サーバ１０３は、ステップ９０３でボリュームを作成した記憶装置システム１０２に対し、ボリューム情報テーブル１２３の更新を指示する命令を発行する。更新指示の命令を受けた記憶装置システム１０２は、ステップ９０３で作成したボリュームに対応する物理ボリュームの物理ボリューム番号、ボリュームへ割り当てたＬＵＮ、ボリュームの記憶容量、ボリュームを割り当てたポートのIPアドレス、ボリュームへＴＣＰコネクションを確立する際に使用するＴＣＰポート番号、ボリュームに割り当てられたオブジェクトＩＤ及びボリュームを割り当てたポートのIPSec機能の有無を含むエントリをボリューム情報テーブル１２３へ追加する。

【００８２】

ただし、図２において、装置ＩＤがStorage2である記憶装置システム１０２の、割り当てIPアドレスが10.10.10.204である物理ポート１２５のように、オブジェクトＩＤが割り当てられていない物理ポート１２５も存在する。そのような物理ポート１２５をボリュームへ割り当てる場合、オブジェクトＩＤの割り当てが行われる。オブジェクトＩＤの割り当て方法として、管理サーバ１０３がシステム管理者へオブジェクトＩＤを入力するよう促し、システムの管理者が手動で管理サーバ１０３へオブジェクトＩＤを入力し、管理サーバ１０３が、そのオブジェクトＩＤを、ボリューム情報テーブル１２３の更新指示を記憶装置システム１０２へ通知する方法がある。また、ボリュームを割り当てられた物理ポートを持つ装置がその物理ポートへ自動的にオブジェクトＩＤを割り当てる方法でも良い（ステップ９０５）。

【００８３】

ステップ９０５の終了後、管理サーバ１０３は、ボリューム作成要求を発行したサーバ１０１や管理者へ対し、ボリューム作成完了通知を発行する。ボリューム作成完了通知には、作成したボリュームへのアクセス経路に関する情報、つまり、作成したボリュームを割り当てた物理ポートのIPアドレス、TCPポート番号、ボリュームへ割り当てたＬＵＮ、ボリュームに割り当てられたオブジェクトＩＤが含まれる（ステップ９０７）。

【００８４】

一方、ステップ９０１でIPSecによる暗号化通信を必要とするボリュームであると判断された場合、管理サーバ１０３は、ポート情報テーブル１３４のフィールド２０５を検索し、IPSec機能を有する物理ポートを特定する。そして、管理サーバ１０３は、特定した物理ポートのIPアドレス及び物理ポートを保持する記憶装置システム１０２の装置ＩＤを特定する。次に管理サーバ１０３は、特定した装置ＩＤでストレージ容量管理テーブル１３５を検索し、特定した装置ＩＤを有する記憶装置システム１０２の空き容量を確認する。そして管理サーバ１０３は、特定した装置ＩＤを有する記憶装置システム１０２の中から、作成が要求されたボリュームの記憶容量以上の空き容量を有する記憶装置システム１０２を特定する（図１０のステップ１００１、１００２）。

【００８５】

次に管理サーバ１０３は、ステップ１００２で特定した記憶装置システム１０２へ、サーバや管理者から要求された記憶容量を有するボリュームの作成を指示する命令を発行する。

ボリューム作成の命令を受信した記憶装置システム１０２は、要求された記憶容量のボリュームを作成する。ボリューム作成を終了した記憶装置システム１０２は、ボリューム作成の終了を管理サーバ１０３へ送信する。

【００８６】
ボリューム作成終了の通知を受信した管理サーバ１０３は、ボリュームを作成した記憶装置システム１０２に対して、作成したボリュームをIPSec機能を有する物理ポートへ割り当てることを指示する命令を発行する。この命令には、管理サーバ１０３がステップ１００２で収集した、特定された記憶装置システム１０２が有するIPSec機能を有する物理ポートに割り振られたIPアドレスの情報が含まれる。
【００８７】
管理サーバ１０３からポート割り当て命令を受けた記憶装置システム１０２は、作成したボリュームを指定された物理ポートへ割り当てる。割当てを終了した記憶装置システム１０２は、その結果を管理サーバ１０３へ通知する（ステップ１００３）。
【００８８】
上記の例では、管理サーバ１０３からボリューム作成命令とポート割り当て命令を別々に発行しているが、それらを一つにまとめた命令を発行する構成も考えられる。そのような構成におけるステップ１００３の動作手順を以下に説明する。
【００８９】
管理サーバ１０３は、ステップ１００２で特定した記憶装置システム１０２へボリューム作成・ポート割り当て命令を発行する。この命令は、サーバや管理者から発行された記憶容量を有するボリュームの作成を指示する命令及び作成したボリュームをIPSec機能を有する物理ポートへ割り当てることを指示する命令を含む。また、この命令には、管理サーバ１０３がステップ１００２で収集した、特定された記憶装置システム１０２が有するIPSec機能を有する物理ポートに割り振られたIPアドレスの情報が含まれる。
【００９０】
ボリューム作成・ポート割り当て命令を受信した記憶装置システム１０２は、要求された記憶容量のボリュームを作成する。ボリューム作成に失敗した場合、記憶装置システム１０２は、管理サーバ１０３へエラー情報を発行する。
【００９１】
ボリューム作成に成功した場合、記憶装置システム１０２は、作成したボリュームを物理ポートへ割り当てる。割り当てを完了した記憶装置システム１０２は、その結果を管理サーバ１０３へ通知する。
【００９２】
ステップ１００２の処理で要求されたボリュームを作成可能な記憶装置システム１０２がシステム上に存在しない場合、IPSec機能を有する物理ポートが無い場合又は記憶装置システム１０２の故障などの理由によりステップ１００３で行われる処理が失敗した場合、管理サーバ１０３は、ボリューム作成要求を発行したサーバ１０１や管理者へエラー情報を通知し、ボリューム作成と割り当て処理を終了する（ステップ１００８）。
【００９３】
ステップ１００２及び１００３の処理が成功した場合、管理サーバ１０３はIPSecアカウント処理を行う。IPSecアカウント処理とは、ＩＫＥ認証に使用するパスワードを、IPSecを使用する装置に登録する処理である。IPSecアカウント処理の詳細は図１１にて説明する。
【００９４】
IPSecアカウント処理の後、管理サーバ１０３は、ストレージ容量管理テーブル１３５及びボリューム情報テーブル１２３の内容の更新を行う。具体的には、管理サーバ１０３は、ストレージ容量管理テーブル１３５の内、ステップ１００３でボリュームを作成した記憶装置システム１０２の空き容量を作成したボリュームの容量分減らし、使用容量を作成したボリュームの容量分増加させる。
【００９５】
また管理サーバ１０３は、ステップ１００３でボリュームを作成した記憶装置システム１０２に対し、ボリューム情報テーブル１２３の更新を指示する命令を発行する。更新指示の命令を受けた記憶装置システム１０２は、ステップ１００３で作成したボリュームに

対応する物理ボリュームの物理ボリューム番号、ボリュームへ割り当てたＬＵＮ、ボリュームの記憶容量、ボリュームに割り当てられたオブジェクトＩＤ、ボリュームに割り当てられたオブジェクトＩＤ及びボリュームを割り当てたポートのIPSec機能の有無を含むエントリをボリューム情報テーブル１２３へ追加する（ステップ１００６）

ステップ１００６又はステップ１００８の実行後、管理サーバ１０３は、ボリューム作成要求を発行したサーバ１０１や管理者へ対し、ボリューム作成完了通知が発行される。以上で、要求されたボリュームのボリューム作成と割り当て処理は完了する。

【００９６】

尚、ボリューム作成完了通知を受けたサーバ１０１は、作成したボリュームをディスクデバイスとして取り扱うため、該ボリュームへデバイス名を付与する。デバイス名を付与する方法は、サーバ１０１上で動作するＯＳが自動的に決めても良いし、サーバ１０１のユーザが手動で決定しても良い。その後、サーバ１０１は、ボリュームへ付与したデバイス名と、ボリューム作成完了通知に含まれたボリュームへアクセスするための経路情報、すなわち、ボリュームに割り当てられたオブジェクトＩＤ、ボリュームへ割り当てたＬＵＮ、ボリュームを割り当てたポートのIPアドレス及びTCPポート番号をパス情報テーブル１１１へ追加する。

【００９７】

尚、サーバ１０１等からのボリューム作成要求にはセキュリティレベル（暗号化の要否）の情報を含めない構成も考えられる。この場合、サーバ１０１が潜在的に要求するセキュリティレベルを判断するため、管理サーバ１０３は、ボリューム作成要求を発行したサーバ１０１がIPSec機能を有する物理ポート１１５ａを有するかどうか判断する。具体的には、管理サーバ１０３が、ボリューム作成要求を発行したサーバ１０１のIPアドレスを元にポート情報テーブル１３４を検索してサーバ１０１がIPSec機能を持つ物理ポート１１５ａを保持するかを特定する。

【００９８】

ボリューム作成要求を発行したサーバ１０１がIPSec機能を持つ物理ポート１１５ａを保持している場合、管理サーバ１０３は、作成が要求されるボリュームへのアクセスに対してセキュリティをかける必要があると判断する。そして、管理サーバ１０３は、作成したボリュームへIPSec機能を持つ物理ポートを割り当てるよう、記憶装置システム１０２に指示する。一方、ボリューム作成要求を発行したサーバ１０１がIPSec機能を持つ物理ポート１１５ａを保持していない場合、管理サーバ１０３は、作成が要求されるボリュームへのアクセスに対してセキュリティをかける必要が無いと判断する。そして、管理サーバ１０３は、作成したボリュームへIPSec機能を持たない物理ポート１１５ｂを割り当てるよう、記憶装置システム１０２へ指示する。

【００９９】

図１１は、管理サーバ１０３が実行するIPSecアカウント処理の詳細な手順例を示す図である。

ボリューム割り当て処理のステップ７０２において、サーバ１０１がボリューム作成要求を発行した場合、IPSecアカウント処理を開始した管理サーバ１０３は、ボリューム作成要求を発行したサーバ１０１が持つ物理ポート１１５及びステップ９０３もしくはステップ１００３でボリュームを割り当てられた物理ポート１２５が持つ認証ＩＤ及びパスワードを、ポート情報テーブル１３４を検索することにより特定する。ここでは、管理サーバ１０３は、物理ポートに割り当てられたIPアドレスに基づいて、各々の物理ポートの認証ＩＤ及びパスワードをポート情報テーブル１３４から検索する。

【０１００】

また、ボリューム割り当て処理のステップ７０２において、管理者がボリューム作成要求を発行した場合、IPSecアカウント処理を開始した管理サーバ１０３は、管理者へ、作成したボリュームへのアクセスを許可するサーバ１０１を指定するよう要求を発行する。管理者からのアクセス許可サーバ情報（アクセスを許可するサーバ１０１の装置ＩＤ）を受けた管理サーバ１０３は、それらのサーバ１０１が持つ物理ポート１１５及びステップ

９０３もしくはステップ１００３でボリュームを割り当てられた物理ポートが持つ認証ＩＤ及びパスワードを、ポート情報テーブル１３４を検索することにより特定する。

【０１０１】

ここでは、管理サーバ１０３は、アクセスを許可すべきサーバ１０１（以下「アクセス許可サーバ１０１」）が持つ物理ポート１１５ａの認証ＩＤ及びパスワードをアクセス許可サーバ１０１の装置ＩＤに基づいて、また、ボリュームを割り当てられた物理ポート１２５が持つ認証ＩＤ及びパスワードを物理ポート１２５ａに割り当てられたIPアドレスに基づいてポート情報テーブル１２２から検索する（ステップ１１０１）。

【０１０２】

各々の物理ポートの認証ＩＤ及びパスワードを特定した管理サーバ１０３は、ステップ１１０１で特定した認証ＩＤとパスワードの内、サーバ１０１が有する物理ポート１１５を用いる際に使用される認証ＩＤ及びパスワードを記憶装置システム１０２が保持するパスワード管理テーブルへ登録する指示を記憶装置システム１０２へ送信する。又管理サーバ１０３は、特定した認証ＩＤとパスワードの内、記憶装置システム１０２が有する物理ポート１２５ａを用いる際に使用される認証ＩＤとパスワードをサーバ１０１が保持するパスワード管理テーブルへ登録する指示をサーバ１０１へ送信する。

【０１０３】

尚、上述の例では、サーバ１０１等が高いセキュリティレベルを要求しない場合、作成したボリュームをIPSec機能を有さない物理ポートに割り当てるように管理サーバ１０３は管理していた。しかし、必ずしもこのようにする必要は無く、サーバ１０１等から高いセキュリティレベルの要求が無くても、管理サーバ１０３が、作成したボリュームをIPSec機能を有する物理ポートに割り当てるよう管理しても良い。この様にするとユーザが要求する以上のセキュリティが確保されてしまうが、空き領域を有する記憶装置システムがIPSec機能を有する物理ボリュームしかない場合でもボリュームの割当てをすることができる。

【０１０４】

上述した第一の実施形態においては、管理サーバ１０３からサーバ１０１へボリュームの作成報告をする際に、ボリュームが作成された記憶装置システム１０２への経路情報も一緒に送付されていた。しかしこれでは、他のサーバ１０１は作成されたボリュームへのアクセスに必要な情報を得られない。したがって、作成されたボリュームはボリューム作成が通知されたサーバ１０１でしか使用できない。

【０１０５】

一方iSCSIでは、サーバが任意の記憶装置システム１０２が有するオブジェクト（ターゲット）を見つける（経路情報を取得する）処理（ディスカバリ）が規定されている。これにより、iSCSIでは、複数のサーバ１０１がボリュームへのアクセスに関する経路情報を共有することが出来る。そこで、第二の実施形態として、第一の実施形態における管理サーバ１０３で、ディスカバリの処理をポート割当ての処理と連携して行う実施形態を考える。

【０１０６】

尚、ディスカバリとは、SCSIイニシエータがSCSIターゲットにログインするために必要な情報を、SCSIターゲットに割り振られたネームを管理する計算機（以下「ネーム管理サーバ」）に問い合わせて得る事を指す。iSCSIに対応するネーム管理プロトコルの例としては、iSNSや、Internet draftである「Finding iSCSI Targets and Name Servers Using SLP」にて規定されるSLP(Service Location Protocol)がある（参考　＜URL：http://www.ietf.org/internet-drafts/draft-ietf-ips-iscsi-slp-06.txt＞）。

【０１０７】

図１２は、第二の実施形態におけるシステム構成例を示した図である。以下、第一の実施形態と異なる点のみ説明する。第二の実施形態における第一の実施形態との主な相違点は、管理サーバ１０３が、第一の実施形態の管理サーバ１０３の構成に加え、ネーム管理サーバの構成を有する点である。尚、以下の説明においては第一の実施形態と同じものに

ついては同じ番号を振るものとする。

【０１０８】

管理サーバ１０３は、第一の実施形態と同様に一般的な計算機であり、プロセッサ、メモリ、及びネットワーク接続部を有する。メモリには、ネットワーク管理プログラム１３２、ネーム管理プログラム１２０１及び構成データベース１３３が格納される。

構成データベース１３３は、ポート情報テーブル１３４、ストレージ容量管理テーブル１３５及びアクセス経路情報テーブル１２０２を有する。

【０１０９】

管理サーバ１０３は、ネットワーク管理プログラム１３２を実行することで、第一の実施形態での処理に加え、ボリューム作成の終了後、作成したボリュームへのアクセス経路（具体的には、アクセスするための必要な情報）及びボリュームへアクセス可能なサーバ１０１のオブジェクトＩＤを、自身が有するアクセス経路情報テーブル１２０２へ登録する処理を行う。これにより、管理サーバ１０３が複数のサーバ１０１に対して同じボリュームへのアクセス経路の情報を提供することが出来る。

【０１１０】

又、管理サーバ１０３は、ネーム管理プログラム１２０１を実行することで、IPネットワーク１０４へ接続するサーバ１０１から受信したSCSIターゲットのディスカバリ要求に対して、アクセス経路情報テーブル１２０２を参照して前記SCSIターゲットへのログインに必要な情報を特定する。そして、管理サーバ１０３は、特定した情報をディスカバリ要求を送信したサーバ１０１へ送信する。

【０１１１】

ここでネーム管理プログラム１２０１としてiSNSを用いた場合、管理サーバ１０３は、ディスカバリ要求で要求されるSCSIターゲットのオブジェクトＩＤ、IPアドレス、ＴＣＰポート番号をサーバ１０１へ通知する。なお、図１２に示した構成例ではネーム管理プログラム１２０１及びアクセス経路情報テーブル１２０２を管理サーバ１０３のメモリ１２９内に格納しているが、それらを管理サーバ１０３とは別の計算機で動作させる構成にしても良い。

【０１１２】

図１３は、アクセス経路情報テーブル１２０２の構成例を示す図である。アクセス経路情報テーブル１２０２は、ネットワーク１０４に接続されたサーバ１０１が、ネットワーク１０４に接続された記憶装置システム１０２が保持するSCSIターゲットへアクセスするために必要な経路情報を管理するテーブルである。アクセス経路情報テーブル１２０２は、ネットワーク１０４に接続される記憶装置システム１０２が有するSCSIターゲットの数分のエントリを有する。

【０１１３】

各エントリは、エントリに対応するSCSIターゲットに割り振られたオブジェクトＩＤを登録するフィールド１３０１、SCSIターゲットに割り振られたIPアドレスを登録するフィールド１３０２、SCSIターゲットのIPアドレスに対応するＴＣＰポート番号を登録するフィールド１３０３及び対応するSCSIターゲットにアクセス可能なサーバ１０１に割り振られているオブジェクトＩＤを格納するフィールド１３０４を有する。

【０１１４】

一つのエントリのフィールド１３０４には、エントリに対応するSCSIターゲットへアクセス可能なサーバ１０１の数分のオブジェクトＩＤが格納される。管理サーバ１０３は、ボリューム作成が行われる度、アクセス経路情報テーブル１２０２を更新する。

【０１１５】

尚、アクセス経路情報テーブル１２０２に保持される情報は、ネーム管理に使用されるプロトコルに依存する。ネーム管理プログラム１２０１がその他の属性を管理する場合、アクセス経路情報テーブル１２０２は該属性に関する情報も格納される。

【０１１６】

図１４は、本実施形態におけるボリューム割り当て処理全体の流れを示す図である。本

実施形態におけるボリューム割り当て処理のうち、ステップ１４０１及び１４０２の処理は第一の実施形態における図８のステップ７０１及び７０２と同じであるので、説明を省略する。ステップ１４０２でサーバ１０１または管理者等からボリューム作成の指示を検出した管理サーバ１０３は、ボリューム作成と割り当て処理１４０３及びアクセス経路通知処理１４０４を実行する。ボリューム作成と割り当て処理１４０３及びアクセス経路通知処理１４０４の詳細は後述する。

【０１１７】

図１５及び図１６は、管理サーバ１０３及び記憶装置システム１０２で実行されるボリューム作成と割り当て処理（図１４のステップ１４０３）の流れを示す図である。尚、第一の実施形態と同様に、サーバ１０１や管理者から管理サーバ１０３に送信されるボリューム作成要求には、ボリュームに必要な記憶容量と要求するセキュリティレベル（ここでは作成するボリュームへアクセスする際にIPSecによる暗号化が必要か否か）の情報が含まれる。尚、第一の実施形態と同様に、セキュリティレベルを管理サーバ１０３がサーバ１０１の物理ポートの特性に応じて決定しても良い。

【０１１８】

図１５において、ステップ１５０１～１５０５及びステップ１５０８で行われる処理は第一の実施形態におけるボリューム作成と割当て処理（図９）のステップ９０１～９０６で行われる処理と同一であるので、説明を省略する。又、図１６において、ステップ１６０１～１６０６及び１６０９で行われる処理は、第一の実施形態におけるボリューム作成と割当て処理（図１０）のステップ１００１～１００６及び１００８で行われる処理と同一であるので、説明を省略する。

【０１１９】

図１５においてステップ１５０５の処理の実行後、管理サーバ１０３は、ステップ１５０３で記憶装置システム１０２へ発行した物理ポートへの割り当て要求に含まれるIPアドレス、ＴＣＰポート番号、及びオブジェクトＩＤをアクセス経路情報テーブル１２０２へ新しいエントリとして登録する。更に、管理サーバ１０３は、ステップ１５０３で作成されたボリュームへアクセス可能なサーバ１０１を決定する。そして管理サーバ１０３は、決定されたサーバ１０１のオブジェクトＩＤを、アクセス経路情報テーブル１２０２に新しく追加されたエントリのフィールド１３０４へ登録する。

【０１２０】

尚、新たに作成されたボリュームへアクセス可能なサーバ１０１を決定する方法は種々存在する。例えば、ボリュームの作成要求を発行したのが管理者である場合には、管理サーバ１０３が管理者へ、作成したボリュームへアクセス可能なサーバ１０１を登録するように促す方法がある。又、ボリュームの作成要求を発行したのがサーバ１０１である場合には、管理サーバ１０３が、作成要求を発行したサーバ１０１を、作成されたボリュームにアクセス可能なサーバ１０１としてアクセス経路情報テーブル１２０２へ登録する方法でも良い。また、ネットワーク１０４に接続されるサーバ１０１を幾つかのグループに分割しておき、管理サーバ１０３が、ボリュームの作成要求を発行したサーバ１０１を含むグループ全てのサーバ１０１を、作成されたボリュームへアクセス可能なサーバ１０１としてアクセス経路情報テーブル１２０２へ登録する方法としても良い（ステップ１５０６）。

【０１２１】

その後、管理サーバ１０３は、ボリューム作成要求を発行したサーバ１０１や管理者へ対し、ボリューム作成完了通知（ここではアクセス経路に関する情報は含まれない）を発行する。以上で、要求されたボリュームが暗号化通信を必要としていない場合のボリューム作成と割り当て処理は完了する。

【０１２２】

図１６において、ステップ１６０６の実行後、管理サーバ１０３は、ステップ１６０３で記憶装置システム１０２へ発行した物理ポートへの割り当て要求に含まれるIPアドレス、ＴＣＰポート番号及びオブジェクトＩＤをアクセス経路情報テーブル１２０２の新しい

エントリとして登録する。

【０１２３】

更に管理サーバ１０３は、ステップ１６０３で作成されたボリュームへアクセス可能なサーバ１０１を決定する。そして管理サーバ１０３は、決定されたサーバ１０１のオブジェクトＩＤを、アクセス経路情報テーブル１２０２の新しく追加されたエントリのフィールド１３０４へ追加する。アクセス可能なサーバ１０１の決定方法は、図１５の説明と同様である（ステップ１６０７）。

【０１２４】

その後、管理サーバ１０３は、ボリューム作成要求を発行したサーバ１０１や管理者へ対し、ボリューム作成完了通知（ここではアクセス経路情報は含まれない）を発行する。

【０１２５】

図１７は、図１４のステップ１４０５で行われるアクセス経路通知処理の手順例を示す図である。管理サーバ１０３は、アクセス経路情報テーブル１２０２を検索して、ステップ１４０３で作成したボリュームへ割り当てたオブジェクトＩＤ、IPアドレス、ＴＣＰポート番号、作成したボリュームへアクセス可能なサーバ１０１を特定する（ステップ１７０１）。

【０１２６】

次に管理サーバ１０３は、ステップ１７０１で特定したオブジェクトＩＤ、IPアドレス及びＴＣＰポート番号を、ステップ１７０１で特定したサーバ１０１へ通知する。管理サーバ１０３がサーバ１０１へオブジェクトＩＤ等を通知する方法として、例えば、iSNSサーバの役割を果たす管理サーバ１０３がSCNをサーバ１０１へ発行し、ネットワーク１０４に接続されたサーバ１０１へディスカバリを要求する方法がある（ステップ１７０２）。

【０１２７】

尚、ネットワーク１０４に接続されたサーバ１０１は、管理サーバ１０３をネーム管理サーバ、本実施形態ではiSNSサーバとして扱う。したがって、サーバ１０１は、自身が使用するターゲットへのアクセス情報を得るため、管理サーバ１０３に対してディスカバリ要求を発行する。

【０１２８】

図１８は、管理サーバ１０３がディスカバリ要求を受け取った際に行う処理（以下「ネーム問い合わせ処理」）の手順例を示した図である。

ディスカバリ要求に基づいた処理を受けつけていない場合、管理サーバ１０３はサーバ１０１からディスカバリ要求を受信したかどうかを監視している（ステップ１８０１）。

【０１２９】

サーバ１０１からディスカバリ要求を受信した管理サーバ１０３は、アクセス経路情報テーブル１２０２を検索し、ディスカバリ要求を発行したサーバ１０１がアクセス可能なSCSIターゲットを特定する。続いて管理サーバ１０３は、ディスカバリ要求を発行したサーバ１０１がアクセス可能なSCSIターゲットのオブジェクトＩＤ、IPアドレス及びＴＣＰポート番号をアクセス経路情報テーブル１２０２から取得する（ステップ１８０２）。

【０１３０】

その後管理サーバ１０３は、ステップ１８０２で取得したオブジェクトＩＤ、IPアドレス及びＴＣＰポート番号を、ディスカバリ要求を発行したサーバ１０１へ通知する（ステップ１８０３）。

【０１３１】

本実施形態によれば、管理サーバ１０３が、記憶装置システム１０３が有するボリュームへのアクセス経路の情報を管理することにより、より柔軟に使用者等に対してボリュームを提供することができる。

【０１３２】

第２の実施形態の一つの変形例として、管理サーバ１０３等が、作成したボリュームに複数の物理ポートを割り当てることで、作成されたボリュームへのアクセス経路を複数提

供する構成がある。例えば、物理ポートとして、IPSecが使用できる物理ポートとIPSecが使用できない物理ポートの双方を、作成された１つのボリュームへ割り当てることができる。つまり、ボリュームへのアクセス経路を複数用意することができる。

【０１３３】

したがって、サーバ１０１が発行するディスカバリ要求に対し、管理サーバ１０３が、複数のアクセス経路の全てをサーバ１０１へ通知したり、複数のアクセス経路のうちの何れか、例えばディスカバリ要求を発行したサーバ１０１がIPSec機能を持つＨＢＡを保持する場合には暗号化可能な物理ポートを使用するアクセス経路を、サーバ１０１がIPSec機能を持つＨＢＡを保持していない場合には暗号化通信が行えない物理ポートを使用するアクセス経路を通知したりすることができる。又サーバ１０１が発行するディスカバリ要求に対し、IPSec機能を有する物理ポートを使用するアクセス経路全てあるいはIPSec機能を有さない物理ポートを使用するアクセス経路全てを通知しても良い。尚、サーバ１０１の物理ポートのIPSec機能の有無は、管理サーバ１０３がポート管理テーブルを参照することで確認できる。

【０１３４】

図１９は、ボリュームに複数のポートを割り当てた場合のボリューム情報テーブル１２３の構成例を示す図である。ボリューム情報テーブル１２３は、基本的には図５で説明したボリューム情報テーブル１２３と同じ構成を有している。ただし、割当てポートのIPアドレスを登録するフィールド１９０４と、割り当てポートのSCSIオブジェクトとＴＣＰコネクションを確立する際に使用するＴＣＰポート番号を登録するフィールド１９０５へそれぞれ複数のポートのIPアドレスとＴＣＰポート番号を登録できる点が図５のボリューム情報テーブル１２３とは異なる。又、IPアドレスが複数登録できることに対応して、登録された各IPアドレスで示される物理ポートがIPSec機能を有するかどうかを示す情報を登録するフィールドが一つのオブジェクトに対して複数用意される点も図６とは異なる。例えば図１９では、物理ボリュームVol. 0に対して、IPSec機能を持つ物理ポートのIPアドレス10.10.10.201と、IPSec機能を持たない物理ポートのIPアドレス10.10.10.202が割り当てられている。

【０１３５】

図２０は、本変形例でのアクセス経路情報テーブル１２０２の構成例を示す図である。本変形例において、アクセス経路情報テーブル１２０２は、図１４で説明したアクセス経路情報テーブル１２０２と異なり、一つのSCSIターゲットに対し複数のアクセス経路の情報を登録することができる。例えば、図２０において、オブジェクトＩＤがiqn.2003-01.com.example:storage１であるSCSIターゲットに対し、IPSec機能を持つポートのIPアドレス10.10.10.201とＴＣＰポート番号３２６０、IPSec機能を持たないポートのIPアドレス10.10.10.202とＴＣＰポート番号３２６０の情報が登録されている。

【０１３６】

本変形例におけるボリューム割り当て処理では、ステップ１４０３で行われるボリューム作成と割り当て処理、及びステップ１４０４で行われるアクセス経路通知処理の手順が変更される。以下、変更点のみを記す。

【０１３７】

先ずボリューム作成と割り当て処理のステップ１５０１においては、判定が行われず、続いてステップ１６０１が実行される。ステップ１６０１、及びステップ１６０２にて行われる処理の内容に変更は無い。

【０１３８】

ステップ１６０３において、管理サーバ１０３は、作成したボリュームをIPSec機能を有する物理ポートと、IPSec機能を有しない物理ポートの両方へ割り当てるよう、記憶装置システム１０２へ命令を発行する。なお、管理サーバ１０３が指定する、作成したボリュームを割り当てる物理ポート数は、2以上の任意の数である。

【０１３９】

ステップ１６０５にて行われるIPSecアカウント処理では、管理サーバ１０３は、ボリ

ュームへ割り当てたIPSec機能を有する物理ポートの認証ＩＤ及びパスワードを、作成したボリュームへのアクセスを許可するサーバ１０１が保持するパスワード管理テーブル１１２へ登録する。ボリュームへ割り当てられたIPSec機能を有する物理ポートが複数ある場合には、それら全ての物理ポートの認証ＩＤ及びパスワードがパスワード管理テーブル１１２へ登録される。

【０１４０】

ステップ１６０５にて行われるボリューム情報テーブル１２３の更新では、ステップ１６０３で記憶装置システム１０２がボリュームへ割り当てた全ての物理ポートのIPアドレス、TCPポート番号がボリューム情報テーブル１２３へ登録される。

【０１４１】

ステップ１６０８で行われるアクセス経路情報テーブル１２０２の更新では、ステップ１６０３で記憶装置システム１０２がボリュームへ割り当てた全ての物理ポートのIPアドレス、ＴＣＰポート番号、及び物理ポートがもつIPSec機能の有無がアクセス経路情報テーブル１２０２へ登録される。

【０１４２】

ステップ１４０５で行われるアクセス経路通知処理のステップ１７０２では、管理サーバ１０３は、ステップ１７０１で特定した作成したボリュームへアクセス可能なサーバ１０１に対し、ディスカバリを要求する。

【０１４３】

管理サーバ１０３は、サーバ１０１からディスカバリ要求を受信した際、アクセス経路情報テーブル１２０２を検索してディスカバリ要求を送信したサーバ１０１がアクセス可能なオブジェクトを特定する。その後管理サーバ１０３は、ポート情報テーブル１３４を検索して、ディスカバリ要求を送信したサーバ１０１が有する物理ポートの特性（ここではIPSec機能の有無）を確認する。そして、管理サーバ１０３は、ディスカバリ要求を送信したサーバ１０１がIPSec機能を持つＨＢＡを保持していた場合には、特定したオブジェクトに割り振られている物理ポートのうち、IPSec機能を持つ物理ポートのIPアドレスとＴＣＰポート番号をサーバ１０１に送信する。一方、サーバ１０１がIPSec機能を持つＨＢＡを保持していなかった場合には、管理サーバ１０３は、特定したオブジェクトに割り振られている物理ポートのうち、IPSec機能を持たない物理ポートのIPアドレスとＴＣＰポート番号をサーバ１０１に送信する。

【０１４４】

図２１は、本変形例における管理サーバ１０３が行うネーム問い合わせ処理の流れを示す図である。ディスカバリ要求に基づいた処理を行っていない場合、管理サーバ１０３はサーバ１０１からディスカバリ要求を受信したかどうかを監視している（ステップ２１０１）。

【０１４５】

サーバ１０１からディスカバリ要求を受信した管理サーバ１０３は、ディスカバリ要求に含まれるサーバ１０１のIPアドレスの情報に基づいてポート情報テーブル１３４を検索し、ディスカバリ要求を送信したサーバ１０１の装置ＩＤを特定する。その後、管理サーバ１０３は、特定した装置ＩＤに基づいてポート情報テーブル１３４を検索し、ディスカバリ要求を送信したサーバ１０１がIPSec機能を持つＨＢＡを保持しているかを特定する（ステップ２１０２、２１０３）。

【０１４６】

ディスカバリ要求を送信したサーバ１０１がIPSec機能を持つＨＢＡを保持していた場合、管理サーバ１０３は、アクセス経路情報テーブル１２０２を検索し、ディスカバリ要求を発行したサーバ１０１がアクセス可能なSCSIターゲットを特定する。続いて管理サーバ１０３は、アクセス経路情報テーブル１２０２を検索し、特定されたSCSIターゲットへ割り当てられている物理ポートのうち、IPSec機能を持つ物理ポートのオブジェクトＩＤ、IPアドレス及びＴＣＰポート番号を特定する（ステップ２１０４）。

【０１４７】

その後、管理サーバ１０３は、ステップ２１０４で特定した情報、具体的には特定された物理ポートのオブジェクトＩＤ、IPアドレス及びTCPポート番号を、ディスカバリ要求を発行したサーバ１０１へ通知し、ステップ２１０１の処理に戻る（ステップ２１０５）。

【０１４８】

一方、ステップ２１０３においてディスカバリ要求を発行したサーバ１０１がIPSec機能を有する物理ポートを有さないと判断された場合、管理サーバ１０３は、アクセス経路情報テーブル１２０２を検索し、ディスカバリ要求を発行したサーバ１０１がアクセス可能なSCSIターゲットを特定する。続いて管理サーバ１０３は、特定したSCSIターゲットに基づいてアクセス経路情報テーブル１２０２を検索し、特定されたSCSIターゲットへ割り当てられている物理ポートのうち、IPSec機能を持たない物理ポートのオブジェクトＩＤ、IPアドレス及びＴＣＰポート番号を特定する（ステップ２１０６）。

【０１４９】

その後、管理サーバ１０３は、ステップ２２０６で特定した情報、具体的には特定された物理ポートのオブジェクトＩＤ、IPアドレス及びTCPポート番号を、ディスカバリ要求を発行したサーバ１０１へ通知し、ステップ２１０１の処理に戻る（ステップ２１０７）。

【０１５０】

第二の実施形態の他の変形例として、ディスカバリ要求を発行するサーバ１０１が、ディスカバリ要求にセキュリティレベルの要求（例えば暗号化の要否）を加える構成もある。このような構成にすることによって、サーバ１０１は、自身が要求するセキュリティレベルを満たすターゲットを管理サーバ１０３に要求することが出来る。

【０１５１】

このような構成は、例えば、iSNSプロトコルに用意された「Vendor Specific Attribute」及び「Vendor Specific Message」を利用することで可能になる。Vender Specific Attributeは、iSNSサーバ（本実施形態では管理サーバ１０３）及びiSNSクライアント（本実施形態ではサーバ１０１や記憶装置システム１０２）に特定の属性を与えるために任意に使用可能なビット列を指す。又Vender Specific Messageは、iSNSサーバとiSNSクライアント間で交換するパケット内に、任意の情報を埋め込んだものである。

【０１５２】

上述の「Vendor Specific Attribute」及び「Vendor Specific Message」を具体的には以下の様に利用する。Vender Specific Attributeに登録する属性情報として「IPSec機能の有無」を定義する。具体的には、iSNSサーバが管理するポート毎、つまり、IPアドレス毎に、IPSecが使用可能であれはビット列にビット１を、IPSecが使用不可能であればビット列にビット０を設定するように決める。また、「暗号化の要否」及び「IPSec機能の有無」の情報をやり取りするVender Specific Messageを定義する。

【０１５３】

上述の定義において、iSNSクライアントがiSNSサーバへ自身のアドレスを登録する際、IPSec機能の使用可否の情報を埋め込んだ「IPSec機能の有無」メッセージをiSNSサーバに送信する。これにより、iSNSサーバは、iSNSクライアントの「IPSec機能の有無」に関する属性情報を収集することができる。その後iSNSクライアントは、iSNSサーバへディスカバリ要求を発行する際、暗号化が必要か否かの情報を埋め込んだ「暗号化の要否」メッセージをディスカバリ要求に含めてiSNSサーバへ送信する。ディスカバリ要求を受けとったiSNSサーバは、収集したiSNSクライアントの「IPSec機能の有無」属性情報を検索し、ディスカバリ要求で暗号化が必要とされていれば、iSNSクライアントがアクセス可能な記憶装置システム１０２のなかで、IPSec機能を持つものだけを通知することが可能となる。

【０１５４】

図２２は、上記他の変形例において、サーバ１０１がセキュリティレベル（ここでは暗号化の要否）を含めてディスカバリ要求を発行する際のネーム問い合わせ処理の手順を示す図である。ディスカバリ要求に基づいた処理を行っていない場合、管理サーバ１０３は

サーバ１０１からディスカバリ要求を受信したかどうかを監視している（ステップ２２０１）。

【０１５５】

ディスカバリ要求を受け取った管理サーバ１０３は、受信したディスカバリ要求に含まれる情報に基づいて、ディスカバリ要求を発行したサーバ１０１が暗号化を必要としているかの判定を行う（ステップ２２０２）。

【０１５６】

ディスカバリ要求を発行したサーバ１０１が暗号化を必要としていると判断された場合、管理サーバ１０３は、上述した変形例（図２１）におけるステップ２１０４及び２１０５と同様の処理を行う。具体的には、管理サーバ１０３は、サーバ１０１がアクセス可能なSCSIターゲットのうち、IPSec機能を有する物理ポートを有するSCSIターゲットの情報をサーバ１０１へ送信する（ステップ２２０３及び２２０４）。

【０１５７】

一方、ディスカバリ要求を発行したサーバ１０１が暗号化を必要としていないと判断された場合、管理サーバ１０３は、上述した変形例（図２１）におけるステップ２１０６及び２１０７と同様の処理を行う。具体的には、管理サーバ１０３は、サーバ１０１がアクセス可能なSCSIターゲットのうち、IPSec機能を有さない物理ポートを有するSCSIターゲットの情報をサーバ１０１へ送信する（ステップ２２０５及び２２０６）。

【０１５８】

尚、ステップ２２０５において、管理サーバ１０３は、IPSecの機能の有無を判断する処理を省略し、単にサーバ１０１がアクセス可能なSCSIターゲットに割り当てられている物理ポートの情報をサーバ１０１へ送信しても構わない。つまり、サーバ１０１から低いセキュリティレベルの要求があった場合には、管理サーバ１０３は、低いセキュリティレベルに対応するSCSIターゲットの物理ポートでも、よりセキュリティレベルが高い物理ポートの情報をサーバに通知しても構わない。

【０１５９】

尚、第一の実施形態においても、管理サーバ１０３は第二の実施形態と同様に、記憶装置システム１０２に対して一つのボリュームに対して複数の物理ポート１２５を割り当てるように指示することが出来る。この場合、ボリューム作成完了をサーバ１０１に通知する際に、管理サーバ１０３は、一つのボリュームに割り当てた複数の物理ポート１２５に関する情報も併せて通知する。通知を受けたサーバ１０１は、サーバ１０１で定めた任意の条件（例えば通知された一方の物理ポート１２５のみを通常使用し、もう一方の物理ポート１２５を代替パス用とする等）に基づいて通知された物理ポート１２５を使用する。

【０１６０】

この場合、サーバ１０１に通知される複数の物理ポートの情報は、双方ともセキュリティレベルが高い物理ポートでも、一部のみセキュリティレベルが高い物理ポートでも、全てセキュリティレベルが低い物理ポートの情報でも良い。例えば、サーバ１０１からの要求が高いセキュリティレベルである場合には、全て高いセキュリティレベルの物理ポートに関する情報が通知される場合や、少なくとも一つの高いセキュリティレベルの物理ポートに関する情報が含まれる場合もある。

【０１６１】

第二の実施形態では、管理サーバ１０３は、ディスカバリ要求を受信した際、サーバ１０１がアクセス可能なボリュームに割り当てられている物理ポートを任意に（あるいはサーバ１０１の物理ポートの種類もしくはサーバ１０１からのセキュリティレベルに応じて）選択し、その選択された物理ポートの情報をサーバ１０１へ送信していた。しかし、第二の実施形態のようにすると、サーバ１０１自身でボリュームへのアクセスについてのセキュリティレベルを随時変更することが難しい。

【０１６２】

そこで、第３の実施形態として、サーバ１０１自身がセキュリティレベルに応じてボリュームへアクセスする物理ポートを選択する構成を考える。

具体的には、管理サーバ１０３が、サーバ１０１からのディスカバリ要求に対し、サーバ１０１がアクセス可能なボリュームに割り当てられている全ての物理ポートのオブジェクトＩＤ、IPアドレス、ＴＣＰポート番号及びIPSec機能の有無の情報をサーバ１０１へ送信する構成とする。

【０１６３】

更に、上述の情報を受信したサーバ１０１は、それらの情報をパス情報テーブル１１１に格納する。そして、サーバ１０１は、パス情報テーブル１１１に格納されているボリュームに対する複数の経路情報を元にして、IPSecによる暗号化が必要な場合のみIPSec機能を持つ物理ポートを選択してアクセスするという構成とする。

【０１６４】

図２３は、本実施形態におけるパス情報テーブル１１１の構成例を示す図である。本実施形態におけるパス情報テーブルは、第一の実施形態で説明したパス情報テーブル１１１（図４）の構成と基本的に同一である。しかし、図４で示したパス情報テーブル１１１とは、デバイス名に割り当てられたIPアドレスが複数の場合がある点及びこれらのIPアドレスに対応する物理ポートのIPSec機能の有無の情報を登録するフィールド２３０６を有する点が異なる。

【０１６５】

例えば、図２３では、デバイス名が/dev/hdaのデバイスへはIPアドレス10.10.10.201、TCPポート番号3260のポートと、IPアドレス10.10.10.202、TCPポート番号３２６０のポートが割り当てられている。IPアドレス10.10.10.201、TCPポート番号3260のポートはIPSec機能を持つ物理ポートであり、IPアドレス10.10.10.202、TCPポート番号３２６０のポートはIPSec機能を持たない物理ポートである。

【０１６６】

図２４は、本実施形態において、サーバ１０１がパス管理プログラム１１０を実行することで行うパス選択処理の手順例を示した図である。サーバ１０１は、ボリュームへのアクセス要求に暗号化が必要である場合にはIPSecを用いた通信経路を使用し、そうでない場合は、IPSecを使用しない通信経路を使用する。

【０１６７】

まずサーバ１０１は、サーバ１０１自身で実行されているプログラムにおいて、ボリュームへのアクセス要求が発行されたか否かの判定を行う（ステップ２４０１）。

ボリュームへのアクセス要求が発行された場合、サーバ１０１は、パス情報テーブル１３０７を検索し、アクセス要求の対象となるボリュームの情報が存在するかを確認する（ステップ２４０２、２４０３）。

【０１６８】

アクセス要求の対象となるボリュームの情報が存在しなかった場合、サーバ１０１は、管理サーバ１０３へのディスカバリ要求を発行する。ディスカバリ要求を受けた管理サーバ１０３は、図２２に示した処理と同様のネーム問い合わせ処理を行う。

【０１６９】

ステップ２４０３でアクセス対象となるボリュームの情報が存在する場合又はステップ２４０４の処理で管理サーバ１０３からアクセス対象となるボリュームの情報を取得した場合、サーバ１０１は、アクセス対象となるボリュームに対してアクセス経路が複数あるか否か判定する（ステップ２４０５）。

【０１７０】

複数経路が存在する場合、サーバ１０１は、ボリュームへのアクセス要求を発行したプログラムが暗号化通信を必要としているか否かの判定を行う。この判定を行う方法として、例えば、ボリュームへのアクセスを行うプログラムが、アクセス要求へ暗号化の要否を含め、それをサーバ１０１が検出する方法や、サーバ１０１の使用者が、プログラム毎に暗号化の要否を事前に設定しておき、その設定に従って判定を行う方法などが考えられる（ステップ２４０６）。

【０１７１】

プログラムが暗号化通信を必要としている場合、サーバ１０１は、複数あるアクセス経路のうち、ターゲット側でIPSec機能を持つ物理ポートが使用されるアクセス経路を選択する。そして、サーバ１０１は、選択したアクセス経路を用いて、アクセス対象となるボリュームを有する記憶装置システム１０２と通信を行う（ステップ２４０９）。

【０１７２】

一方、プログラムが暗号化通信を必要としていない場合、サーバ１０１は、複数あるアクセス経路のうち、ターゲット側でIPSec機能を持たない物理ポートが使用されるアクセス経路を選択する。そして、サーバ１０１は、選択したアクセス経路を用いて、アクセス対象となるボリュームを有する記憶装置システム１２と通信を行う（ステップ２４０８）。

【０１７３】

又、ステップ２４０５でアクセス経路が複数無いと判定された場合、サーバ１０１は、アクセス対象であるボリュームに対する唯一のアクセス経路を用いて記憶装置システム１０２と通信を行う。

【０１７４】

尚、第一の実施形態においても、第三の実施形態と同様のことを行うことができる。この場合、サーバ１０１は、ボリューム作成完了通知を受信する際に、複数のアクセス経路に関する情報を受け取り、パス情報テーブルへ登録する。

【図面の簡単な説明】

【０１７５】

【図１】第一の実施形態におけるシステム構成例を示す図である。
【図２】ポート情報テーブルの構成例を示す図である。
【図３】ストレージ容量テーブルの構成例を示す図である。
【図４】パス情報テーブルの構成例を示す図である。
【図５】ボリューム情報テーブルの構成例を示す図である。
【図６】パスワード管理テーブルの構成例を示す図である。
【図７】ボリューム割り当て処理の手順例を示す図である。
【図８】構成情報管理処理の手順例を示す図である。
【図９】ボリューム作成と割り当て処理の手順例を示す図である。
【図１０】ボリューム作成と割り当て処理の手順例を示す図である。
【図１１】IPSecアカウント処理の手順例を示す図である。
【図１２】実施形態２におけるシステム構成例を示す図である。
【図１３】アクセス経路情報テーブルの構成例を示す図である。
【図１４】実施形態２におけるボリューム割り当て処理全体の手順例を示す図である。
【図１５】実施形態２におけるボリューム作成と割り当て処理の手順を示す図である。
【図１６】実施形態２におけるボリューム作成と割り当て処理の手順を示す図である。
【図１７】アクセス経路通知処理の手順を示す図である。
【図１８】ネーム問い合わせ処理の手順を示す図である。
【図１９】ボリューム情報テーブルの構成例を示す図である。
【図２０】アクセス経路情報テーブルの構成例を示す図である。
【図２１】ネーム問い合わせ処理の手順例を示す図である。
【図２２】ネーム問い合わせ処理の手順例を示す図である。
【図２３】パス情報テーブルの構成例を示す図である。
【図２４】パス選択処理の手順例を示す図である。

【符号の説明】

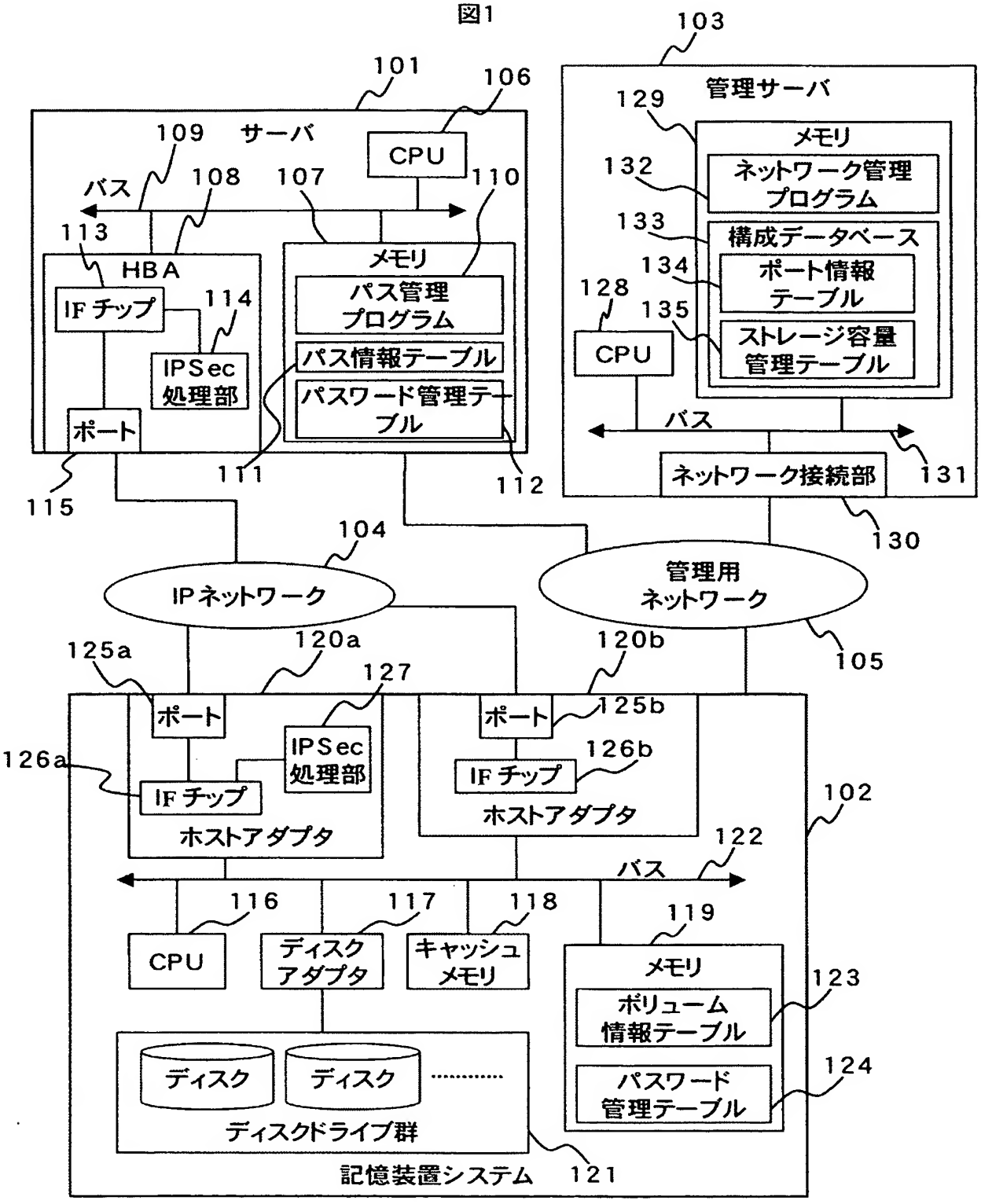
【０１７６】

１０１…サーバ、１０２…記憶装置システム、１０３…管理サーバ、１０４…IPネットワ

ーク、１０５…管理用ネットワーク。

【書類名】図面
【図１】

図1


103
管理サーバ
129
メモリ
132
ネットワーク管理プログラム
133
構成データベース
134
ポート情報テーブル
135
ストレージ容量管理テーブル
128
CPU
バス
ネットワーク接続部
131
130
101
106
109
サーバ
CPU
バス
108
107
110
113
HBA
IFチップ
114
IPSec処理部
ポート
メモリ
パス管理プログラム
パス情報テーブル
パスワード管理テーブル
111
112
115
104
IPネットワーク
管理用ネットワーク
105
125a
120a
120b
127
ポート
ポート
125b
126a
IPSec処理部
126b
IFチップ
IFチップ
ホストアダプタ
ホストアダプタ
102
122
バス
116
117
118
119
CPU
ディスクアダプタ
キャッシュメモリ
メモリ
123
ボリューム情報テーブル
124
パスワード管理テーブル
ディスク
ディスク
ディスクドライブ群
記憶装置システム
121

【図２】

図2

201 装置ID	202 オブジェクトID	203 IPアドレス	204 ノード種別	205 IPSec機能の有無	206 認証ID	207 パスワード
Host 1	iqn.2003-01.com.example.host1	10.10.10.101	ホスト	有り	10.10.10.101	aaaaaa
Host 2	iqn.2003-02.com.example.host2	10.10.10.102	ホスト	無し	－	－
Host 3	iqn.2003-03.com.example.host3	10.10.10.103	ホスト	有り	10.10.10.103	cccccc
Storage 1	iqn.2003-03.com.example.storage1	10.10.10.201	ストレージ	有り	10.10.10.201	dddddd
	iqn.2003-04.com.example.storage1	10.10.10.202	ストレージ	無し	－	－
Storage 2	iqn.2003-05.com.example.storage2	10.10.10.203	ストレージ	有り	10.10.10.203	ffffff
	-	10.10.10.204	ストレージ	無し	－	－
Storage 3	iqn.2003-06.com.example.storage3	10.10.10.205	ストレージ	有り	10.10.10.205	hhhhhh

【図３】

図3

301 装置ID	302 空き容量	303 使用容量
Storage 1	10TB	5TB
Storage 2	20TB	12TB
Storage 3	8TB	2TB

【図４】

図4

401 デバイス名	402 オブジェクトID	403 LUN	404 IPアドレス	405 TCP ポート番号
/dev/sda	iqn.2003-03.com.examplestorage1	0	10.10.10.201	3260
/dev/sdb		1		
/dev/sdc	iqn.2003-05.com.examplestorage2	0	10.10.10.203	3261
/dev/sdd		1		

【図５】

図5

501 物理ボリューム番号	502 LUN	503 容量	504 割り当てポートのIPアドレス	505 TCP ポート番号	506 割り当てポートのオブジェクトID	508 IPSec機能の有無
Vol. 0	0	200GB	10.10.10.201	3260	iqn.2003-01.com.examplestorage1	有り
Vol. 1	1	400GB				
Vol. 2	2	350GB				
Vol. 3	3	600GB	10.10.10.202	3261	iqn.2003-04.com.examplestorage1	無し

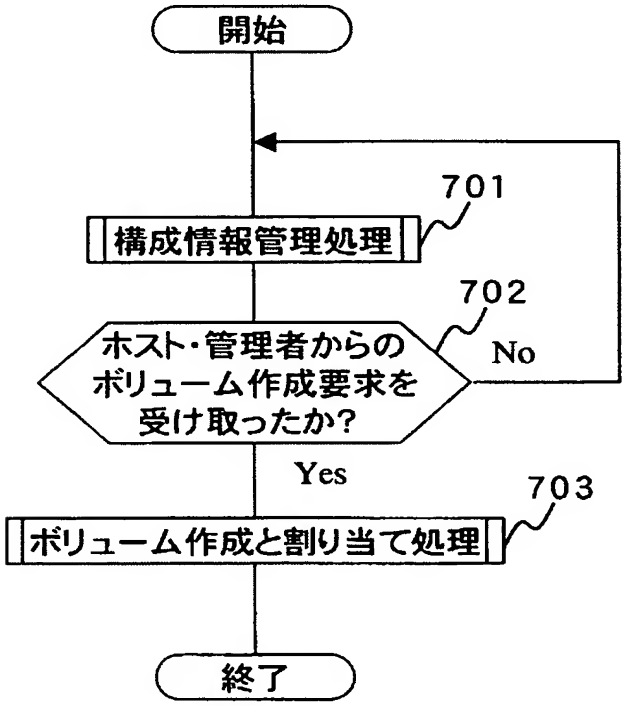
【図６】

図6

601 認証ID	602 パスワード
10.10.10.201	dddddd
10.10.10.202	eeeeee

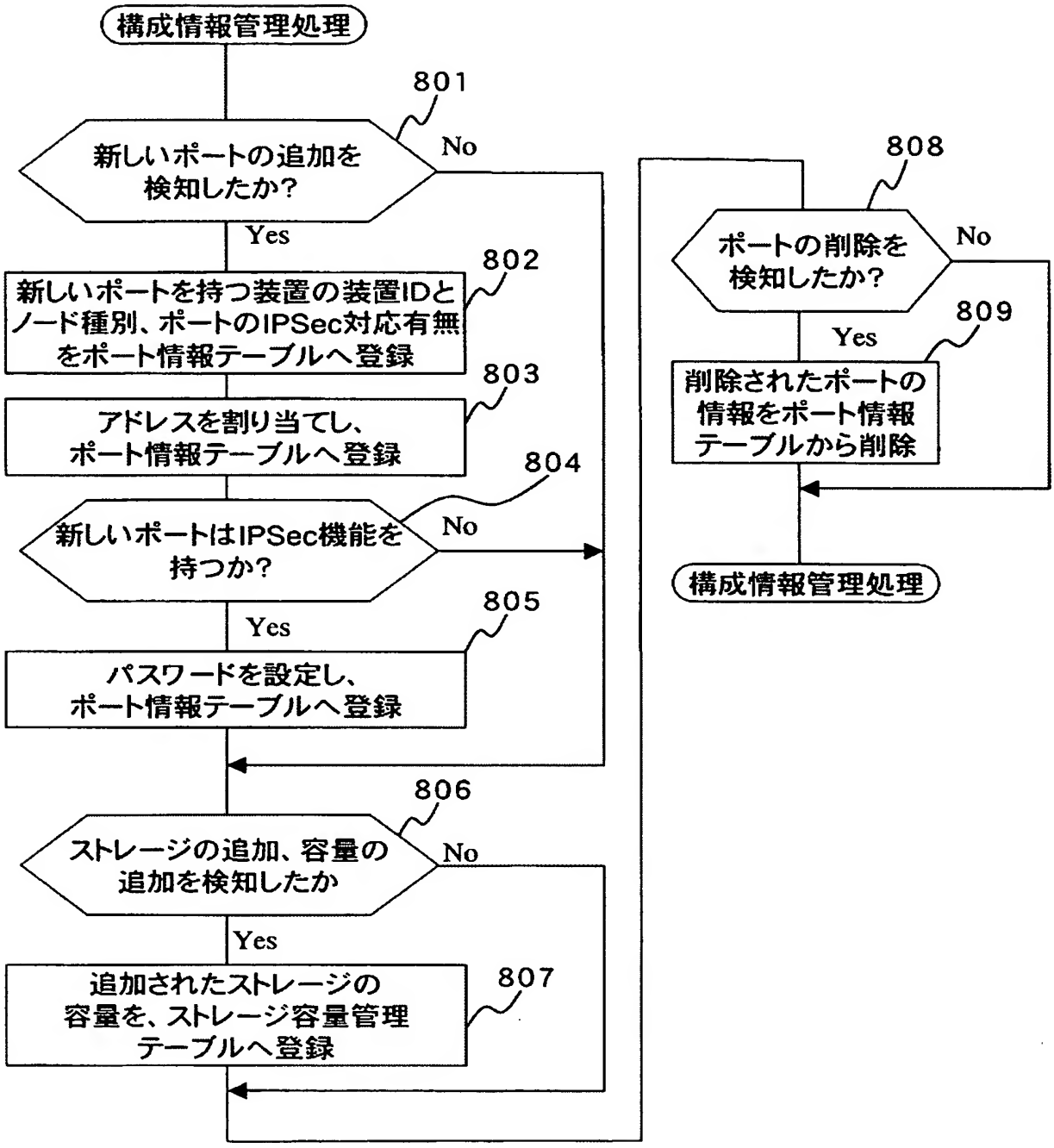
【図７】

図7



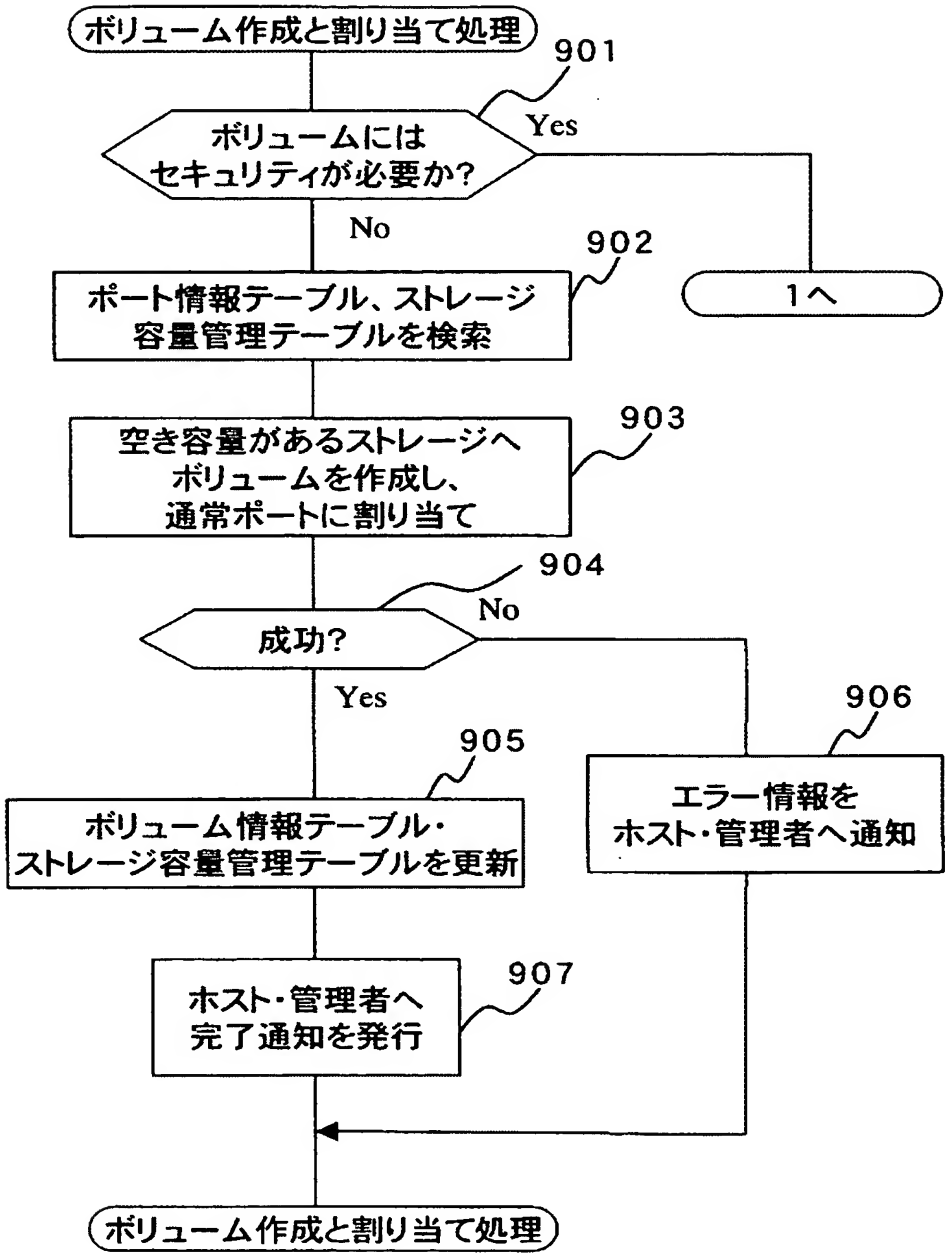
【図８】

図8


構成情報管理処理
801
新しいポートの追加を検知したか?
No
Yes
802
新しいポートを持つ装置の装置IDとノード種別、ポートのIPSec対応有無をポート情報テーブルへ登録
803
アドレスを割り当てし、ポート情報テーブルへ登録
804
新しいポートはIPSec機能を持つか?
No
Yes
805
パスワードを設定し、ポート情報テーブルへ登録
806
ストレージの追加、容量の追加を検知したか
No
Yes
807
追加されたストレージの容量を、ストレージ容量管理テーブルへ登録
808
ポートの削除を検知したか?
No
Yes
809
削除されたポートの情報をポート情報テーブルから削除
構成情報管理処理

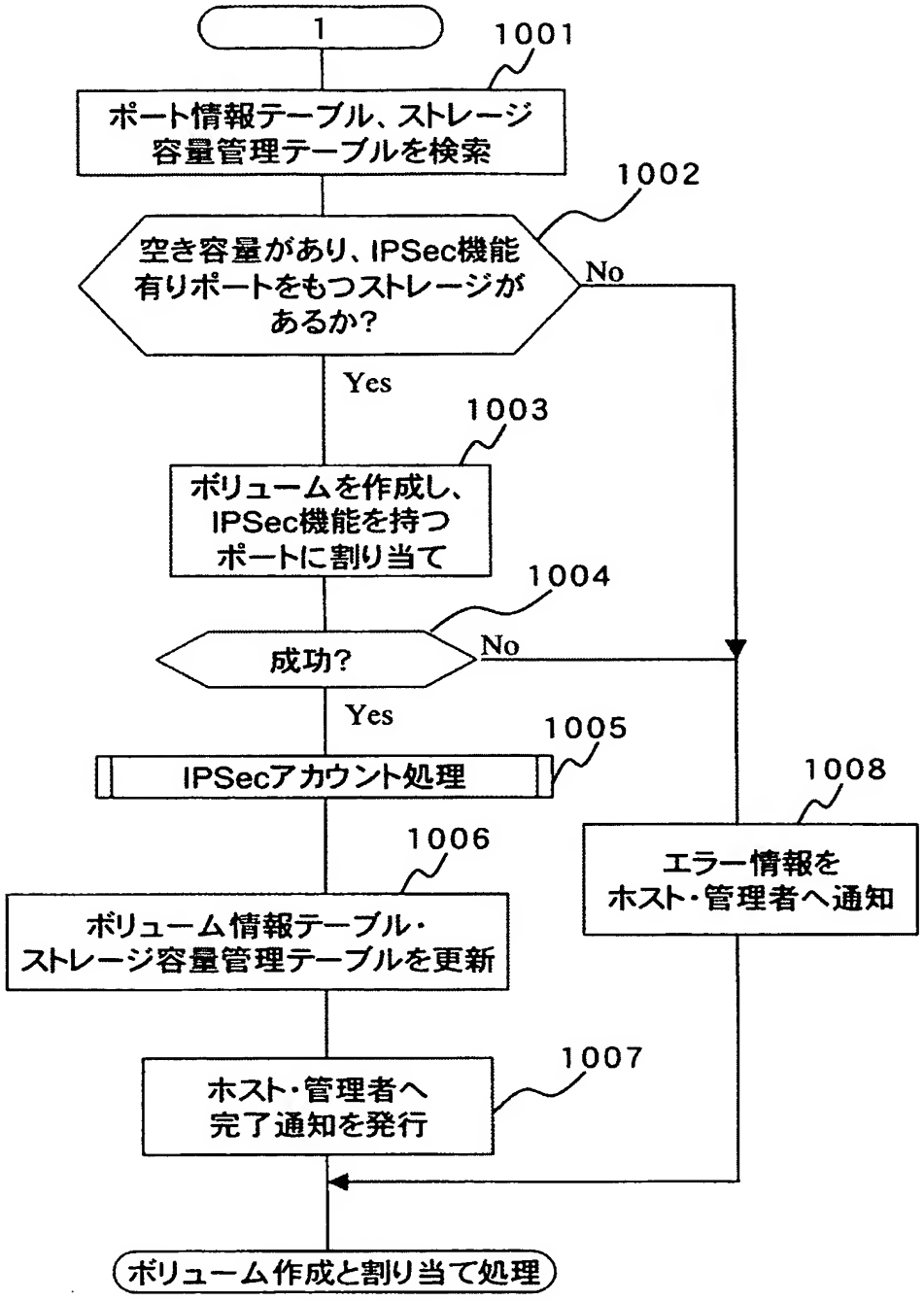
【図９】

図9


ボリューム作成と割り当て処理
901
ボリュームには
セキュリティが必要か?
Yes
No
902
ポート情報テーブル、ストレージ
容量管理テーブルを検索
1へ
903
空き容量があるストレージへ
ボリュームを作成し、
通常ポートに割り当て
904
No
成功?
Yes
906
905
エラー情報を
ホスト・管理者へ通知
ボリューム情報テーブル・
ストレージ容量管理テーブルを更新
907
ホスト・管理者へ
完了通知を発行
ボリューム作成と割り当て処理

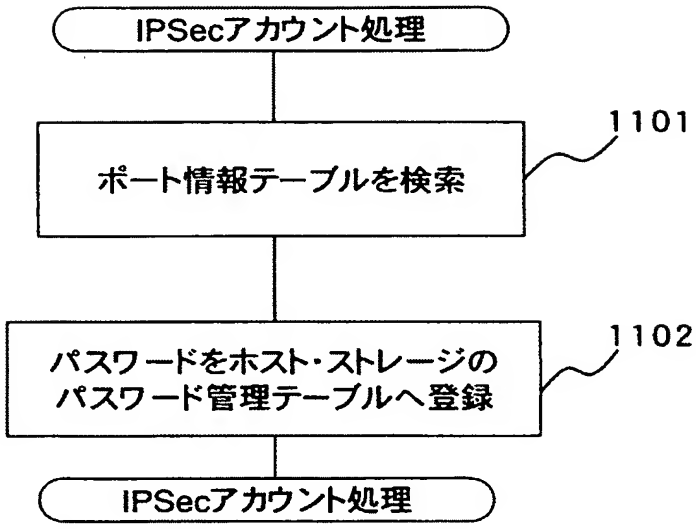
【図１０】

図10


1
1001
ポート情報テーブル、ストレージ容量管理テーブルを検索
1002
空き容量があり、IPSec機能有りポートをもつストレージがあるか?
No
Yes
1003
ボリュームを作成し、IPSec機能を持つポートに割り当て
1004
成功?
No
Yes
1005
IPSecアカウント処理
1008
エラー情報をホスト・管理者へ通知
1006
ボリューム情報テーブル・ストレージ容量管理テーブルを更新
1007
ホスト・管理者へ完了通知を発行
ボリューム作成と割り当て処理

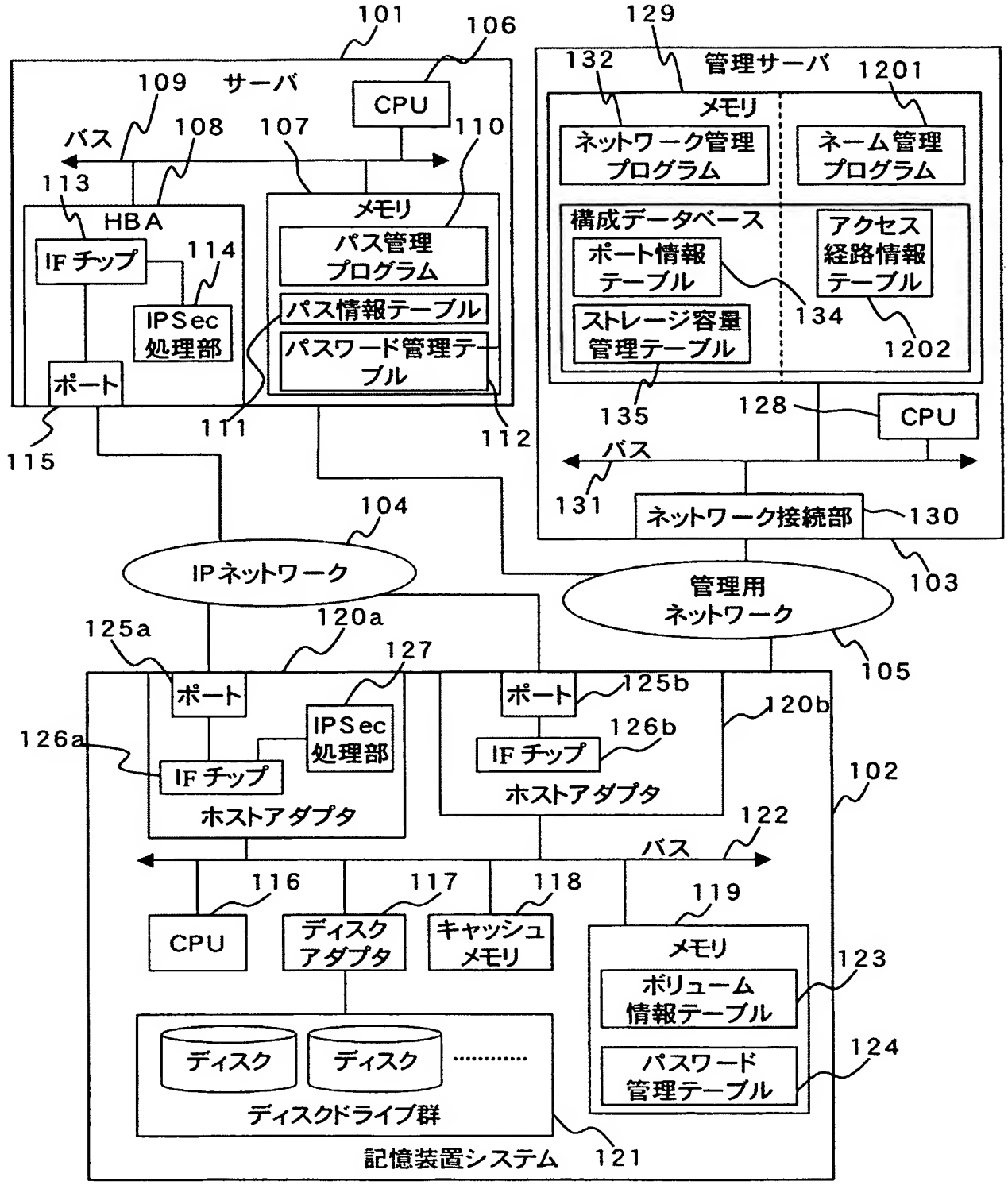
【図１１】

図11


IPSecアカウント処理
1101
ポート情報テーブルを検索
1102
パスワードをホスト・ストレージの
パスワード管理テーブルへ登録
IPSecアカウント処理

【図１２】

図12


101
106
129
サーバ
CPU
管理サーバ
132
1201
109
バス
108
107
110
メモリ
ネットワーク管理プログラム
ネーム管理プログラム
113
HBA
メモリ
構成データベース
アクセス経路情報テーブル
IFチップ
114
パス管理プログラム
ポート情報テーブル
IPSec処理部
パス情報テーブル
134
ストレージ容量管理テーブル
1202
ポート
パスワード管理テーブル
135
128
CPU
111
112
115
バス
131
ネットワーク接続部
130
104
IPネットワーク
管理用ネットワーク
103
125a
120a
127
105
ポート
ポート
125b
120b
IPSec処理部
126a
126b
IFチップ
IFチップ
ホストアダプタ
ホストアダプタ
102
122
バス
116
117
118
119
CPU
ディスクアダプタ
キャッシュメモリ
メモリ
123
ボリューム情報テーブル
124
ディスク
ディスク
パスワード管理テーブル
ディスクドライブ群
記憶装置システム
121

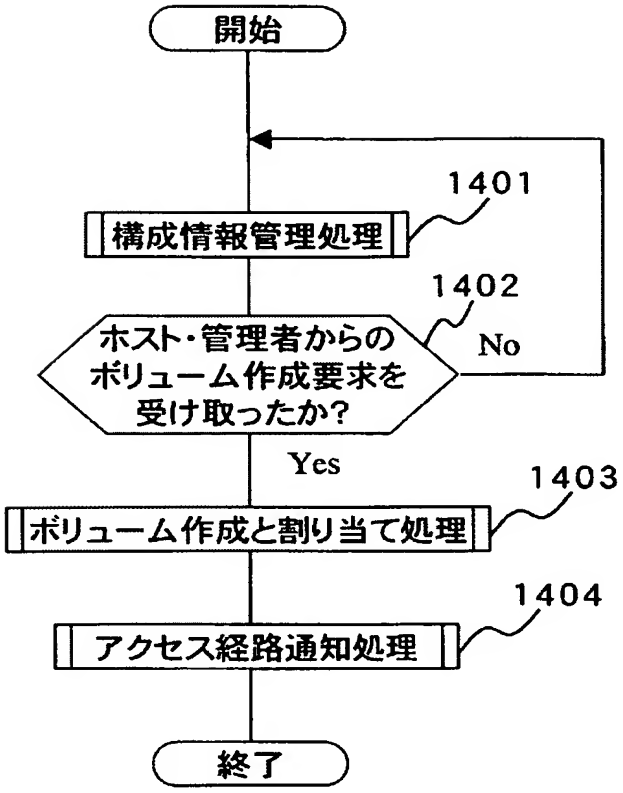
【図１３】

図13

1301 オブジェクトID	1302 IPアドレス	1303 TCPポート番号	1304 アクセス可能なホストのオブジェクトID
iqn.2003-03.com.example:storage1	10.10.10.201	3260	iqn.2003-01.com.example:host1
			iqn.2003-02.com.example:host2
iqn.2003-04.com.example:storage1	10.10.10.202	3261	iqn.2003-01.com.example:host1
			iqn.2003-02.com.example:host2
iqn.2003-05.com.example:storage2	10.10.10.203	3261	iqn.2003-01.com.example:host1
iqn.2003-06.com.example:storage3	10.10.10.204	3260	iqn.2003-02.com.example:host2

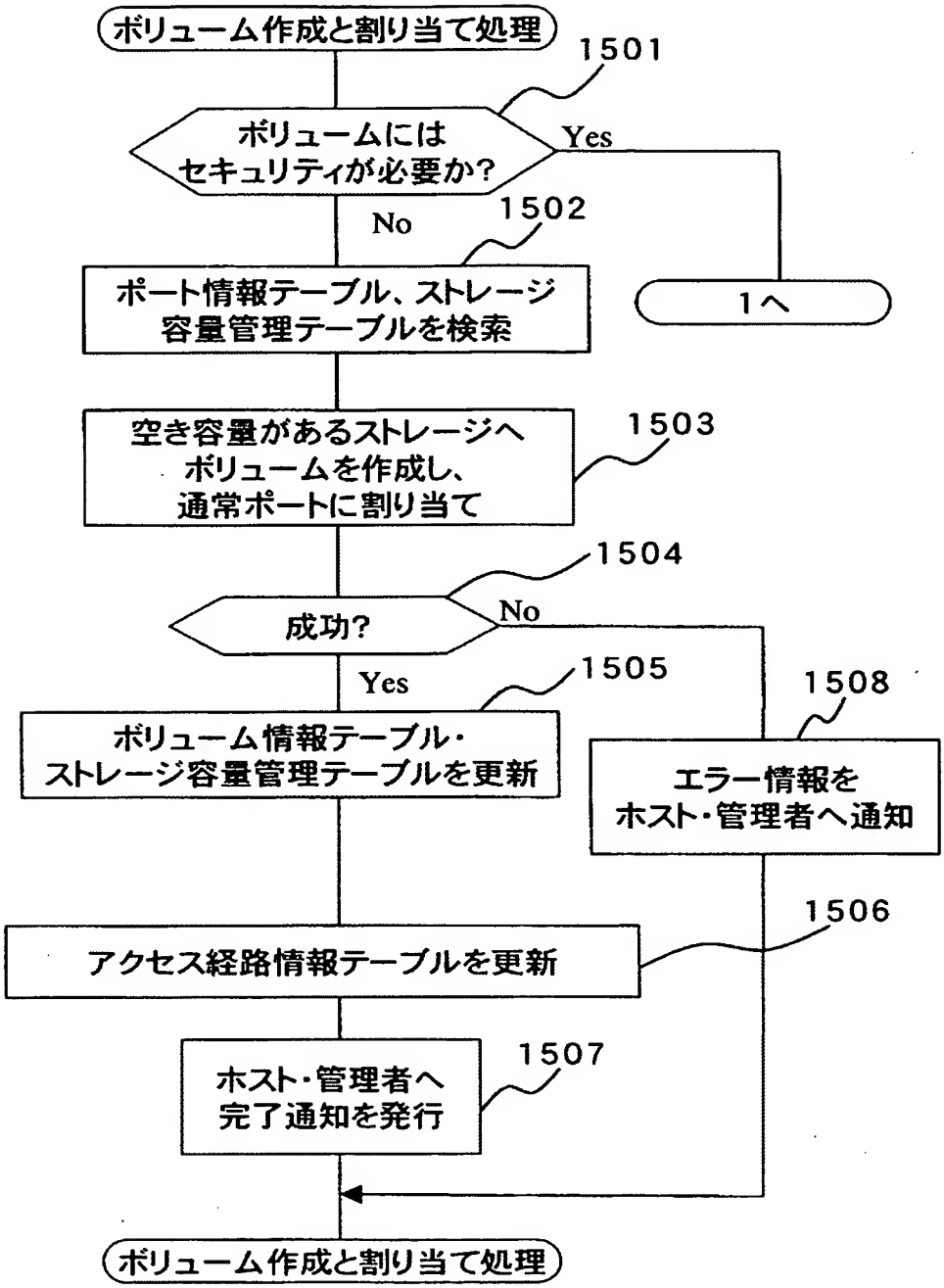
【図１４】

図14


開始
1401
構成情報管理処理
1402
ホスト・管理者からの
ボリューム作成要求を
受け取ったか?
No
Yes
1403
ボリューム作成と割り当て処理
1404
アクセス経路通知処理
終了

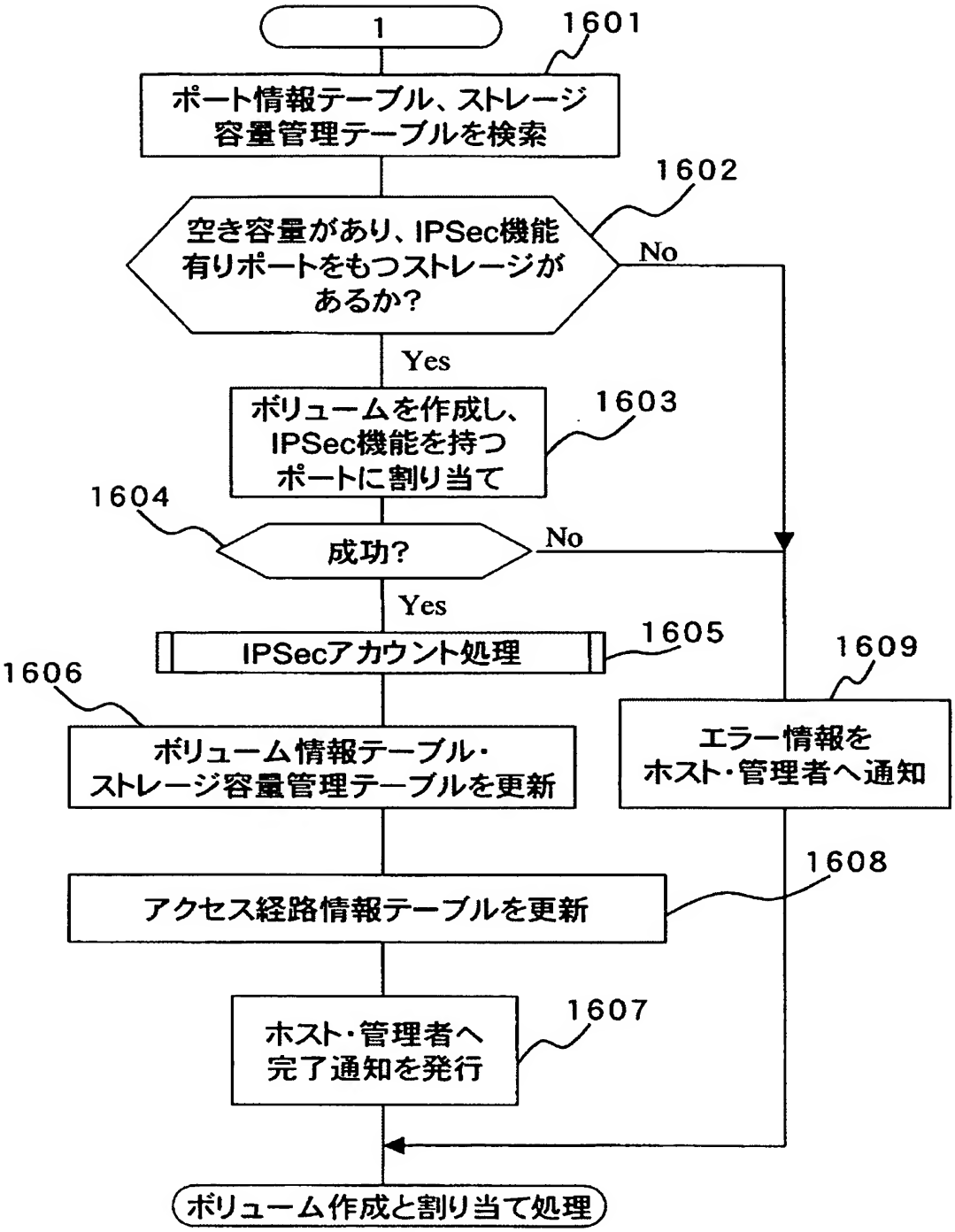
【図１５】

図15


ボリューム作成と割り当て処理
1501
ボリュームには
セキュリティが必要か?
Yes
No
1502
ポート情報テーブル、ストレージ
容量管理テーブルを検索
1へ
空き容量があるストレージへ
ボリュームを作成し、
通常ポートに割り当て
1503
1504
成功?
No
Yes
1505
1508
ボリューム情報テーブル・
ストレージ容量管理テーブルを更新
エラー情報を
ホスト・管理者へ通知
1506
アクセス経路情報テーブルを更新
ホスト・管理者へ
完了通知を発行
1507
ボリューム作成と割り当て処理

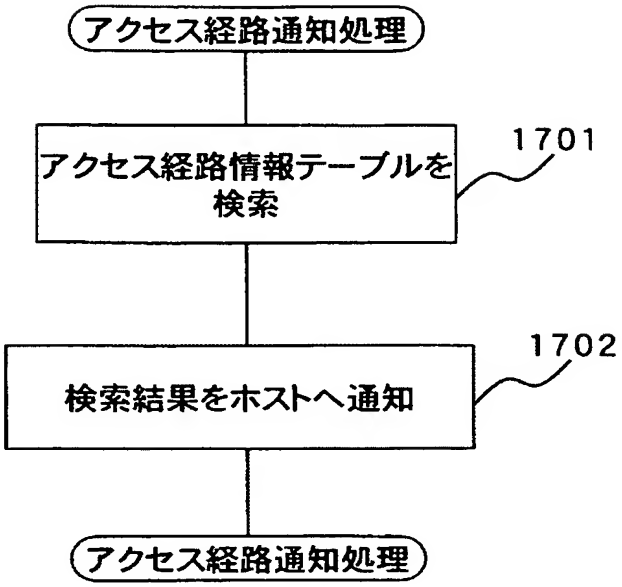
【図１６】

図16


1
1601
ポート情報テーブル、ストレージ容量管理テーブルを検索
1602
空き容量があり、IPSec機能有りポートをもつストレージがあるか?
No
Yes
ボリュームを作成し、IPSec機能を持つポートに割り当て
1603
1604
成功?
No
Yes
IPSecアカウント処理
1605
1606
1609
ボリューム情報テーブル・ストレージ容量管理テーブルを更新
エラー情報をホスト・管理者へ通知
1608
アクセス経路情報テーブルを更新
ホスト・管理者へ完了通知を発行
1607
ボリューム作成と割り当て処理

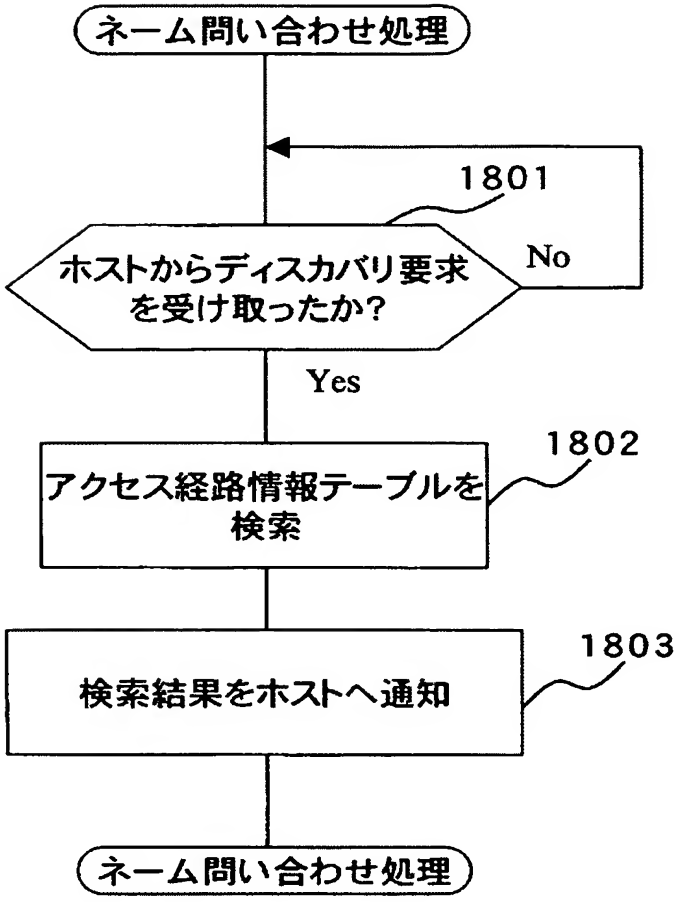
【図１７】

図17


アクセス経路通知処理
アクセス経路情報テーブルを検索
1701
検索結果をホストへ通知
1702
アクセス経路通知処理

【図１８】

図18


ネーム問い合わせ処理
1801
ホストからディスカバリ要求を受け取ったか?
No
Yes
1802
アクセス経路情報テーブルを検索
1803
検索結果をホストへ通知
ネーム問い合わせ処理

【図１９】

図19

1901 物理ボリューム番号	1902 LUN	1903 容量	1904 割り当てポートのIPアドレス	1905 TCPポート番号	1906 割り当てポートのオブジェクトID	1907 IPSec機能の有無
Vol. 0	0	200GB	10.10.10.201	3260	iqn.2003-01.com.examplestorage1	有り
			10.10.10.202	3260		無し
Vol. 1	1	350GB	10.10.10.201	3260		有り
			10.10.10.202	3260		無し
Vol. 2	2	600GB	10.10.10.203	3261	iqn.2003-02.com.examplestorage1	無し
			10.10.10.204	3260		有り
Vol. 3	3	400GB	10.10.10.203	3261		無し
			10.10.10.204	3260		有り

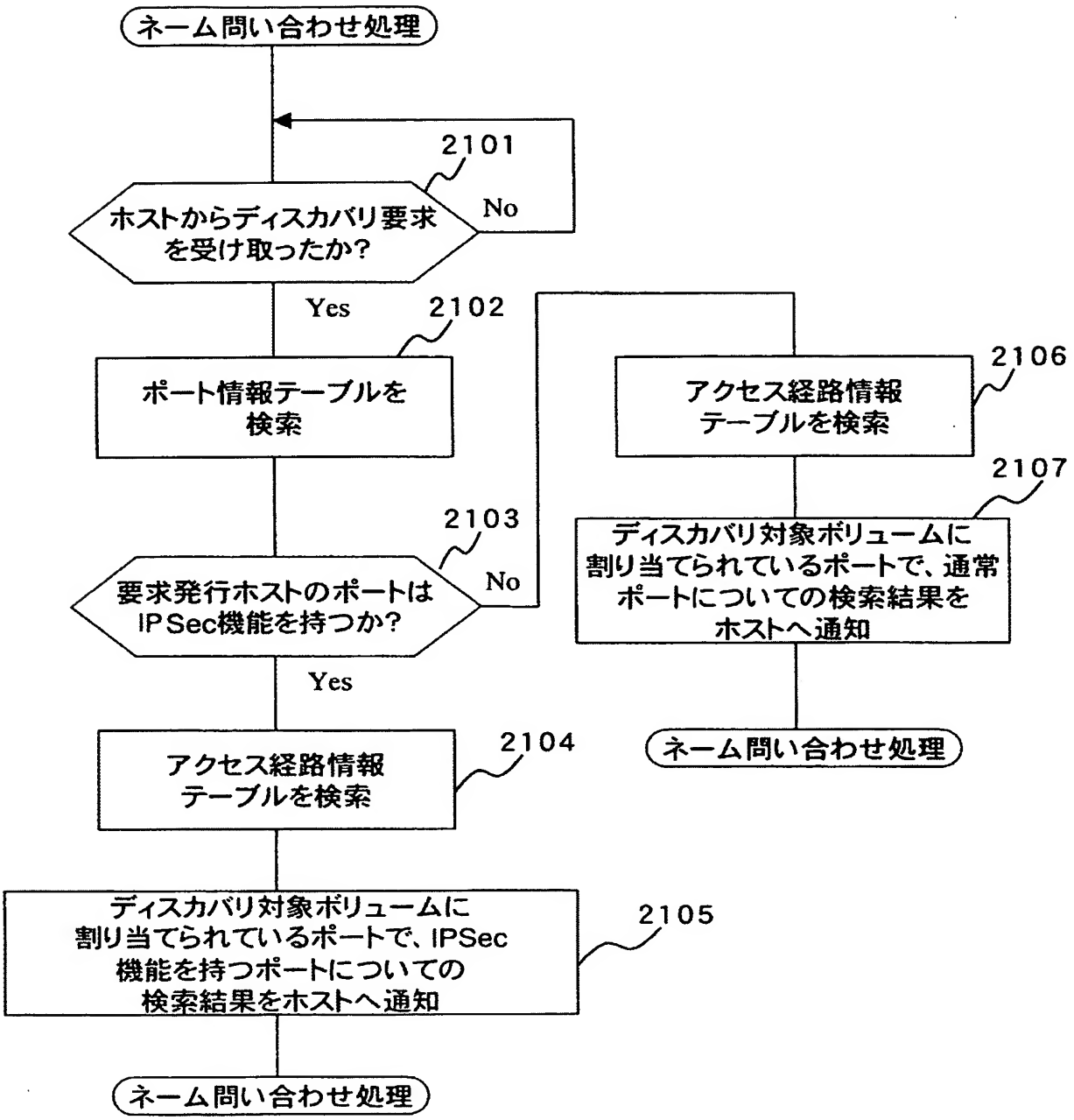
【図２０】

図20

2001 割り当てポートのオブジェクトID	2002 割り当てポートのIPアドレス	2003 TCPポート番号	2004 IPSec機能の有無	2005 アクセス可能なホストのオブジェクトID
iqn.2003-01.com.examplestorage1	10.10.10.201	3260	無し	iqn.2003-01.com.examplehost1
	10.10.10.202	3260	有り	iqn.2003-02.com.examplehost2
iqn.2003-02.com.examplestorage1	10.10.10.203	3261	無し	iqn.2003-01.com.examplehost1
	10.10.10.204	3260	有り	iqn.2003-02.com.examplehost2
iqn.2003-03.com.examplestorage2	10.10.10.205	3261	有り	iqn.2003-01.com.examplehost1

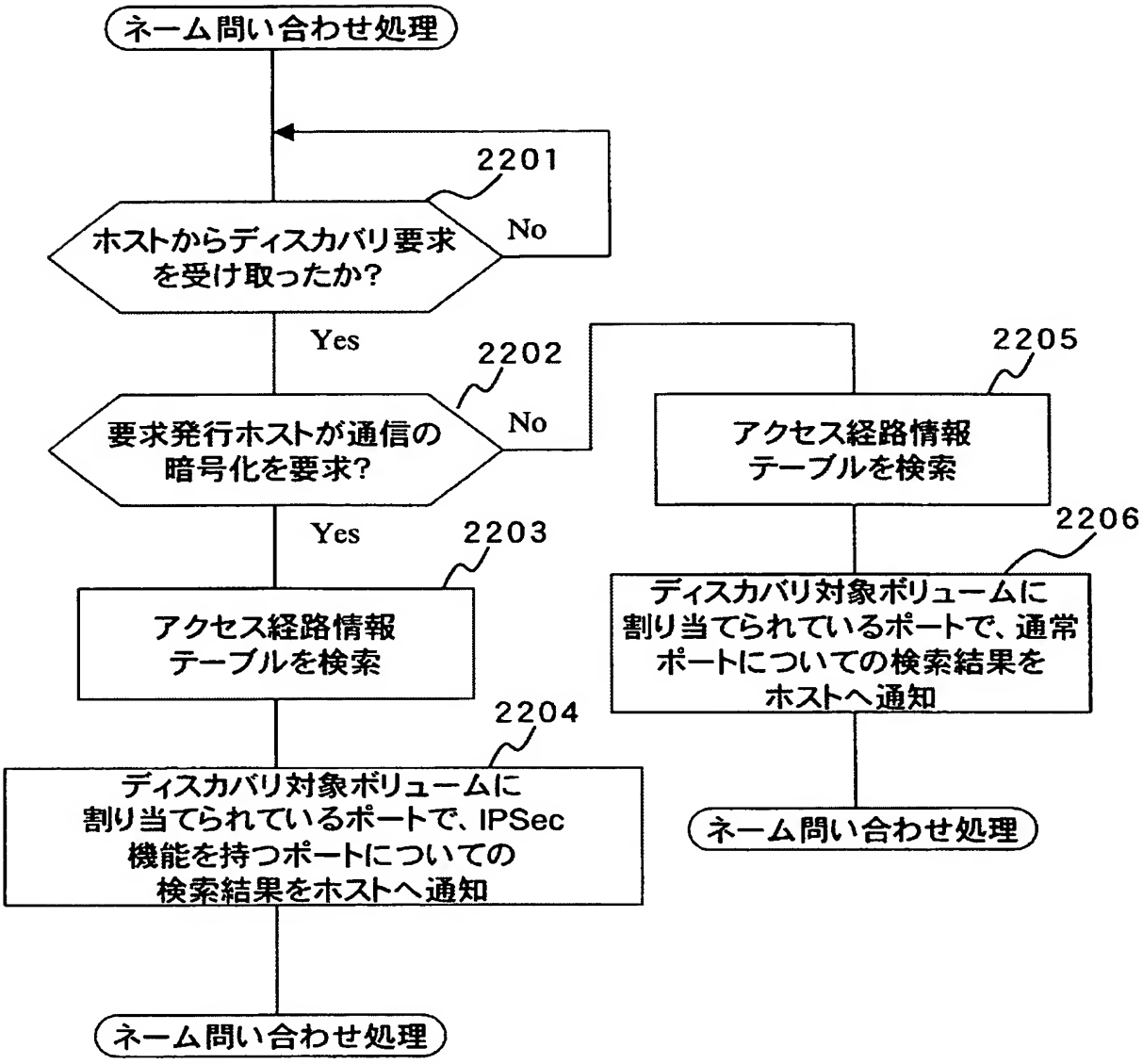
【図２１】

図21


ネーム問い合わせ処理
2101
ホストからディスカバリ要求を受け取ったか?
No
Yes
2102
ポート情報テーブルを検索
2103
要求発行ホストのポートはIPSec機能を持つか?
No
Yes
2104
アクセス経路情報テーブルを検索
2105
ディスカバリ対象ボリュームに割り当てられているポートで、IPSec機能を持つポートについての検索結果をホストへ通知
ネーム問い合わせ処理
2106
アクセス経路情報テーブルを検索
2107
ディスカバリ対象ボリュームに割り当てられているポートで、通常ポートについての検索結果をホストへ通知
ネーム問い合わせ処理

【図２２】

図22


ネーム問い合わせ処理
2201
ホストからディスカバリ要求を受け取ったか?
No
Yes
2202
要求発行ホストが通信の暗号化を要求?
No
Yes
2203
アクセス経路情報テーブルを検索
2204
ディスカバリ対象ボリュームに割り当てられているポートで、IPSec機能を持つポートについての検索結果をホストへ通知
ネーム問い合わせ処理
2205
アクセス経路情報テーブルを検索
2206
ディスカバリ対象ボリュームに割り当てられているポートで、通常ポートについての検索結果をホストへ通知
ネーム問い合わせ処理

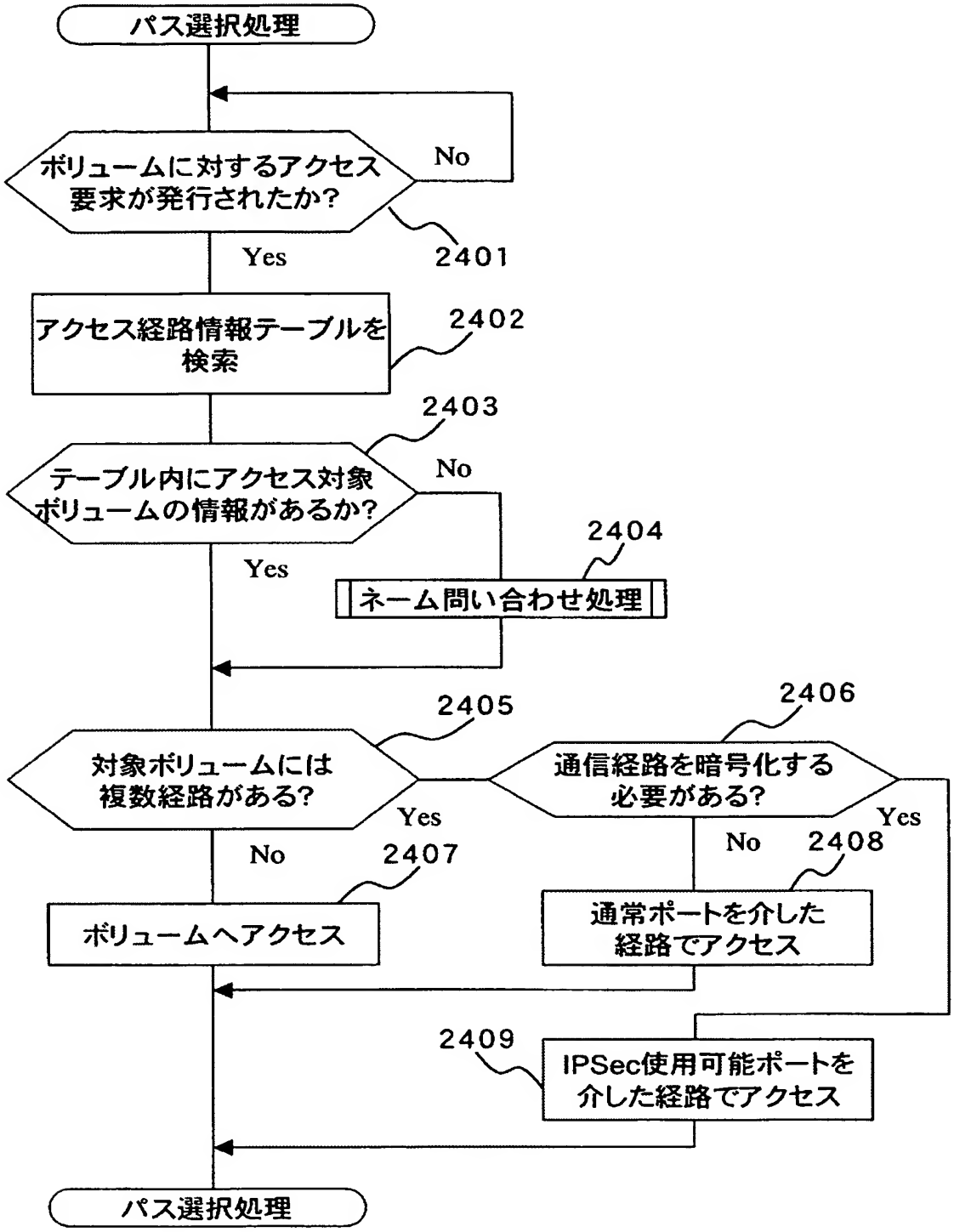
【図２３】

図23

2301 デバイス名	2302 オブジェクトID	2303 LUN	2304 IPアドレス	2305 TCPポート番号	2306 IPSec機能の有無
/dev/sda	iqn.2003-01.com.example:storage1	0	10.10.10.201	3260	無し
			10.10.10.202	3260	有り
/dev/sdb	iqn.2003-02.com.example:storage1	2	10.10.10.203	3261	無し
			10.10.10.204	3260	有り
/dev/sdc	iqn.2003-03.com.example:storage2	1	10.10.10.205	3261	有り

【図２４】

図24


パス選択処理
ボリュームに対するアクセス要求が発行されたか?
No
Yes
2401
アクセス経路情報テーブルを検索
2402
テーブル内にアクセス対象ボリュームの情報があるか?
2403
No
Yes
2404
ネーム問い合わせ処理
対象ボリュームには複数経路がある?
2405
Yes
No
2407
ボリュームへアクセス
通信経路を暗号化する必要がある?
2406
Yes
No
2408
通常ポートを介した経路でアクセス
2409
IPSec使用可能ポートを介した経路でアクセス
パス選択処理

【書類名】要約書
【要約】
【課題】
セキュアな通信を行いたいボリュームへ、IPSec使用可能なポートを割り当てる作業を自動化できない。
【解決手段】
管理サーバが、物理ポートが持つセキュリティ機能の有無を管理し、その情報を元にボリューム作成後殿物理ポートへボリュームを割り当てるかを自動的に決定し、割り当て作業を行う。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００４－０５２７００
受付番号	５０４００３１７９５１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１６年　３月　１日

＜認定情報・付加情報＞

【提出日】　平成16年 2月27日

特願２００４－０５２７００

出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所